MaaS360® by Fiberlink

MaaS360 for Mobile Devices

Getting the Most Guide

Fiberlink Communications Corporation

1787 Sentry Parkway West

Blue Bell, PA 19422

July 2013

010

MaaS360 by Fiberlink

Table of Contents

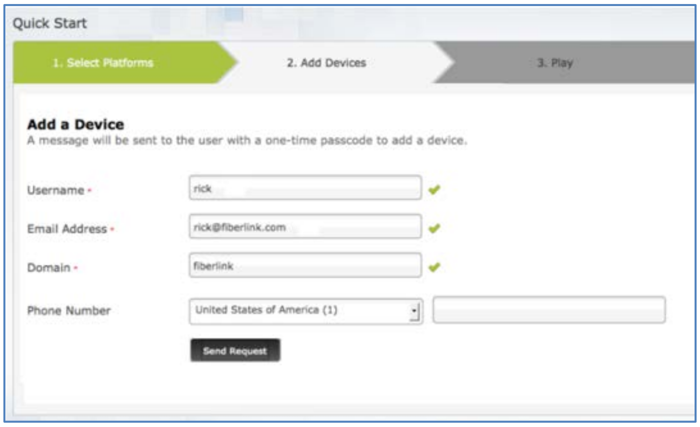
Overview

Businesses and employees are using mobile devices in ways not envisioned before. Personal device ownership and usage is growing rapidly. MaaS360 for Mobile Devices is a cloud-based multi-tenant platform that provides enhanced management of your iOS and Android devices.

You can register for a 30 day trial of the MaaS360 Mobile Device Management solution via the MaaS360 website at http://www.maas360.com.

After registering, a success message will appear. Click the green button to continue.

The Quick Start screens will walk you through setting up your account and enrolling devices.



Quick Start

Add a Device

A message will be sent to the user with a one-time passcode to add a device.

Username • rick ✓

Email Address • rick@fiberlink.com ✓

Domain • fiberlink ✓

Phone Number United States of America (1)

Note: *The account you create as part of your trial will continue into Production if you purchase MaaS360. The devices you enroll as part of your trial will not need to be enrolled again.*

You will receive a welcome email containing important information about your trial. Be sure to keep this information, in case you need support later.

Step 1: Select Platforms

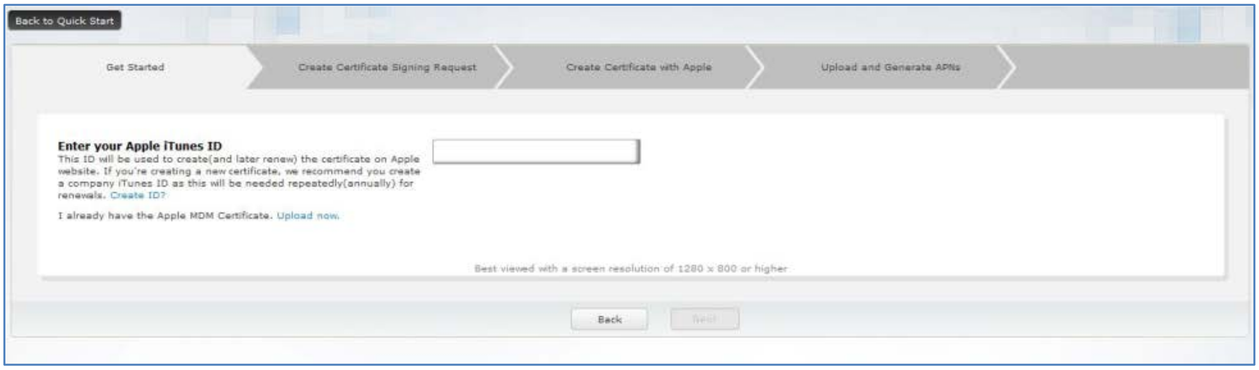
MaaS360 is automatically configured to support Android, Windows Phone and BlackBerry devices. If these are the only devices you will be using, click **Start without iOS** to move to the next step, **Add Devices**.

If you will be using iOS devices, Apple requires you to have an Apple Push Notification service (APNs) certificate. MaaS360 will walk you through the process of obtaining this certificate:

1. Click **Setup iOS Now**. The Safari, Chrome and Firefox web browsers are recommended for this process.
2. Enter a corporate AppleID. You must use the same AppleID every year when renewing your APNs certificate.

   If you don’t have an AppleID, hover over **Create ID?** and click **Apple Website.** This will take you to a page where you can create a corporate AppleID.

   Enter the AppleID and click **Next**.


Back to Quick Start
Get Started
Create Certificate Signing Request
Create Certificate with Apple
Upload and Generate APNs
Back
Next

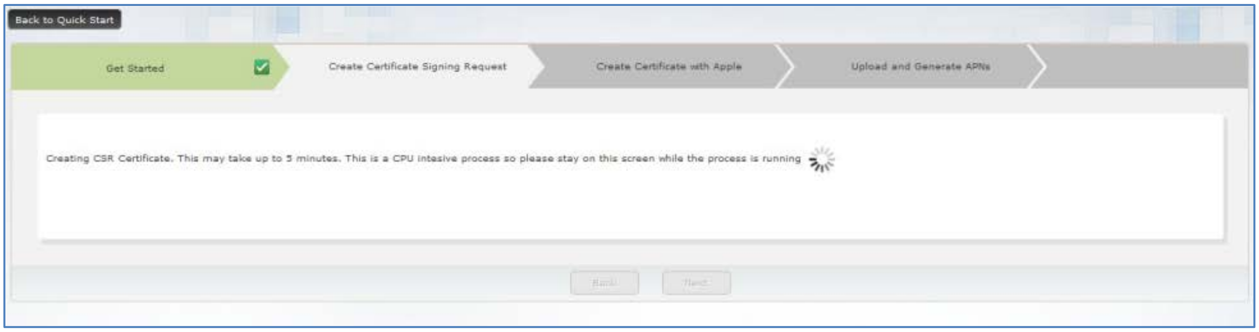
Enter your Apple iTunes ID
This ID will be used to create(and later renew) the certificate on Apple website. If you're creating a new certificate, we recommend you create a company iTunes ID as this will be needed repeatedly(annually) for renewals. Create ID?

I already have the Apple MDM Certificate. Upload now.

Best viewed with a screen resolution of 1280 x 800 or higher

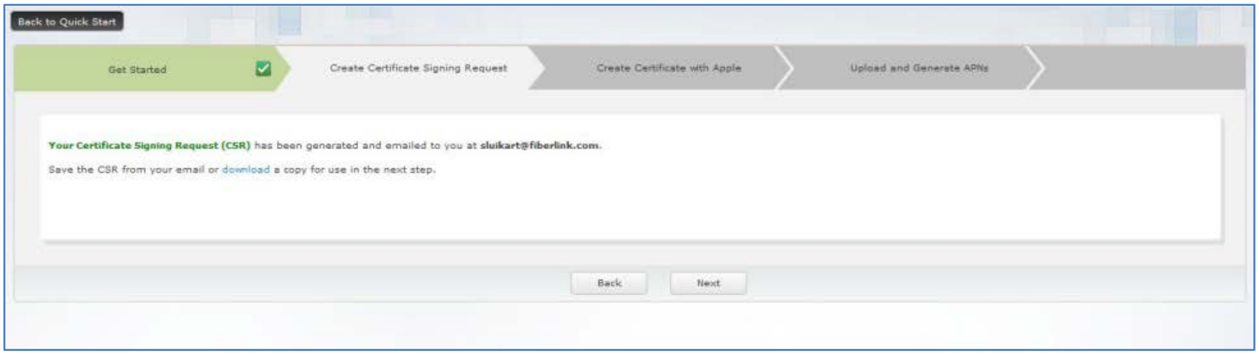
Note: *We strongly recommend that this AppleID belong to your company and not an individual. The AppleID you use to set up your devices is the same one you will need to renew your certificate each year. If you use a personal AppleID and the person leaves your company, you will need to create a new AppleID at renewal time and re-enroll all of your iOS devices using it.*

3. The Certificate Signing Request (CSR) will be generated automatically. This process can take up to 5 minutes. Please remain on this page or you will have to redo the previous steps.



Creating CSR Certificate. This may take up to 5 minutes. This is a CPU intesive process so please stay on this screen while the process is running

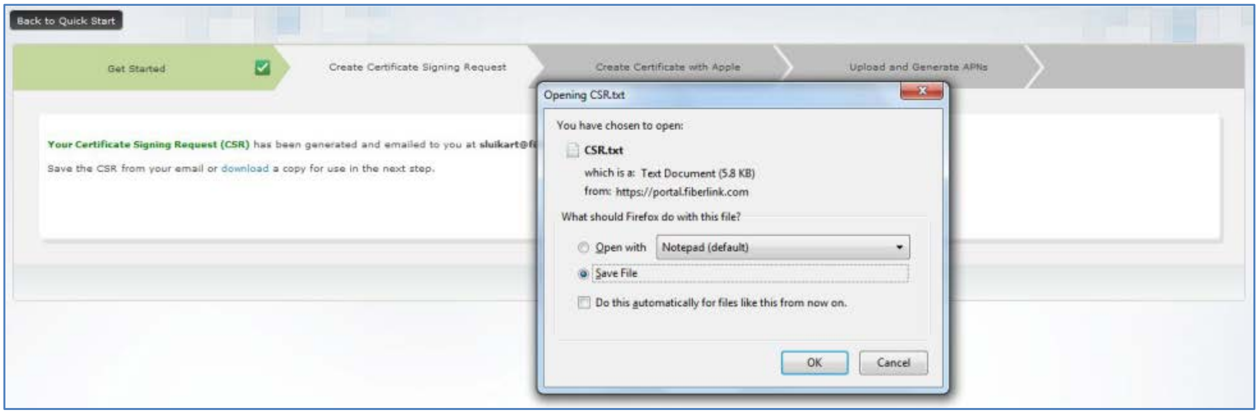
4. The CSR will be emailed to the specified account. You can also click the **download** link to upload it right away.



Your Certificate Signing Request (CSR) has been generated and emailed to you at **sluikart@fiberlink.com**.

Save the CSR from your email or download a copy for use in the next step.

5. After clicking the **download** link, you will be able to save the file. Saving it will put it in your **Downloads** folder by default.


Back to Quick Start
Get Started
Create Certificate Signing Request
Create Certificate with Apple
Upload and Generate APNs

Your Certificate Signing Request (CSR) has been generated and emailed to you at **sluikart@fi**

Save the CSR from your email or download a copy for use in the next step.

Opening CSR.txt

You have chosen to open:

CSR.txt

which is a: Text Document (5.8 KB)

from: https://portal.fiberlink.com

What should Firefox do with this file?

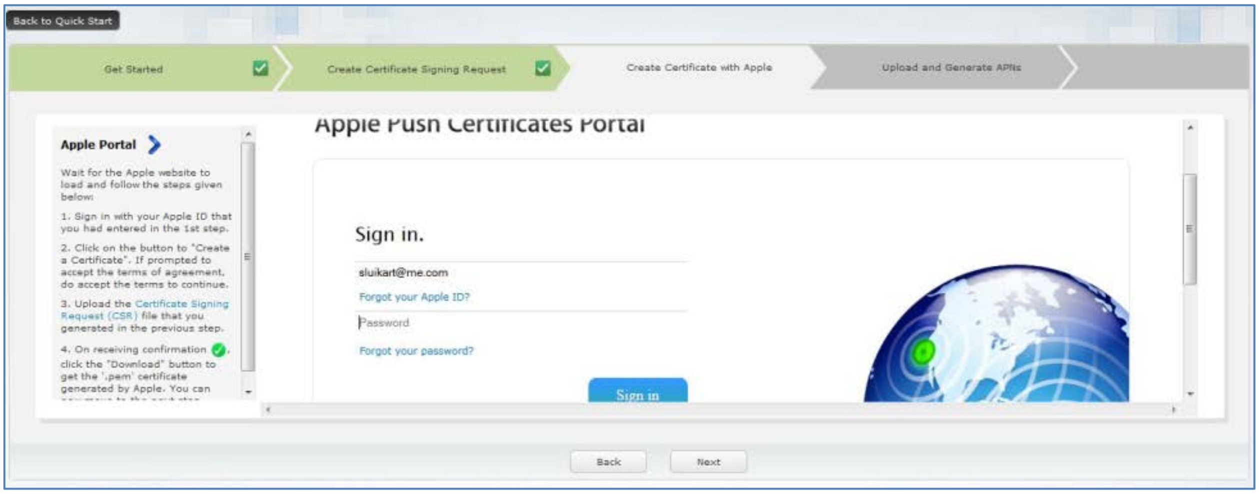
○ Open with Notepad (default)

● Save File

□ Do this automatically for files like this from now on.

6. Enter the AppleID you used in Step 2 and the password, and then click **Sign in**.

   To skip the steps necessary to generate a PEM file, click **Next**. Continue with Step #12.


Back to Quick Start
Get Started
Create Certificate Signing Request
Create Certificate with Apple
Upload and Generate APNs
Apple Portal
Apple Push Certificates Portal
Sign in.
Sign in
Back
Next

Wait for the Apple website to load and follow the steps given below:

1. Sign in with your Apple ID that you had entered in the 1st step.
2. Click on the button to "Create a Certificate". If prompted to accept the terms of agreement, do accept the terms to continue.
3. Upload the Certificate Signing Request (CSR) file that you generated in the previous step.
4. On receiving confirmation ✓, click the "Download" button to get the '.pem' certificate generated by Apple. You can

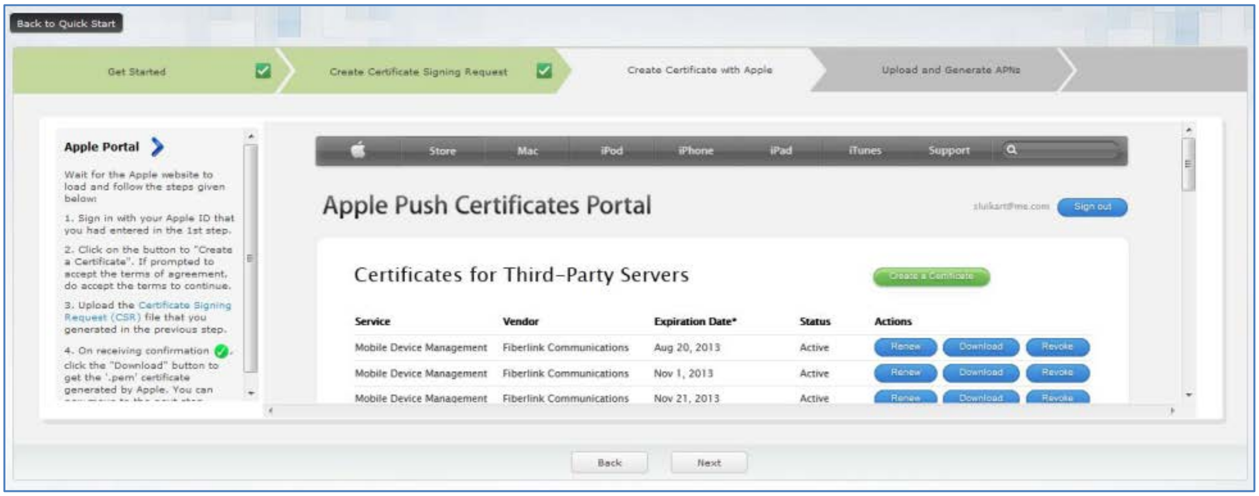
sluikart@me.com

Forgot your Apple ID?

Password

Forgot your password?

7. Click the green **Create a Certificate** button.



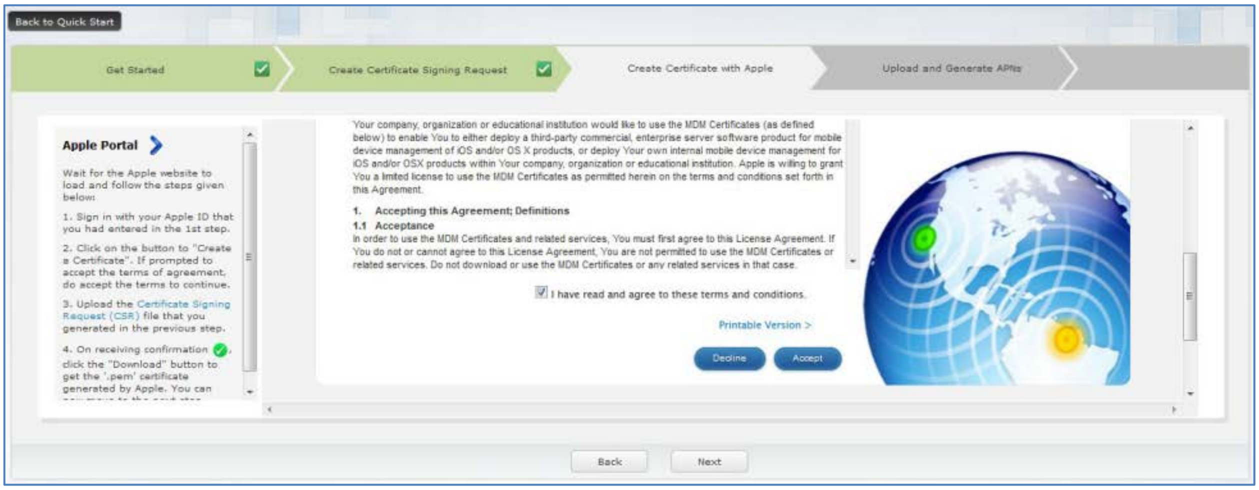
Wait for the Apple website to load and follow the steps given below:

1. Sign in with your Apple ID that you had entered in the 1st step.
2. Click on the button to "Create a Certificate". If prompted to accept the terms of agreement, do accept the terms to continue.
3. Upload the Certificate Signing Request (CSR) file that you generated in the previous step.
4. On receiving confirmation ✓, click the "Download" button to get the '.pem' certificate generated by Apple. You can

Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	Fiberlink Communications	Aug 20, 2013	Active	Renew Download Revoke
Mobile Device Management	Fiberlink Communications	Nov 1, 2013	Active	Renew Download Revoke
Mobile Device Management	Fiberlink Communications	Nov 21, 2013	Active	Renew Download Revoke

8. Check the box next to **I have read and agree to these terms and conditions** and click **Accept**.



Apple Portal

Wait for the Apple website to load and follow the steps given below:

1. Sign in with your Apple ID that you had entered in the 1st step.

2. Click on the button to "Create a Certificate". If prompted to accept the terms of agreement, do accept the terms to continue.

3. Upload the Certificate Signing Request (CSR) file that you generated in the previous step.

4. On receiving confirmation ✓, click the "Download" button to get the '.pem' certificate generated by Apple. You can

Your company, organization or educational institution would like to use the MDM Certificates (as defined below) to enable You to either deploy a third-party commercial, enterprise server software product for mobile device management of iOS and/or OS X products, or deploy Your own internal mobile device management for iOS and/or OSX products within Your company, organization or educational institution. Apple is willing to grant You a limited license to use the MDM Certificates as permitted herein on the terms and conditions set forth in this Agreement.

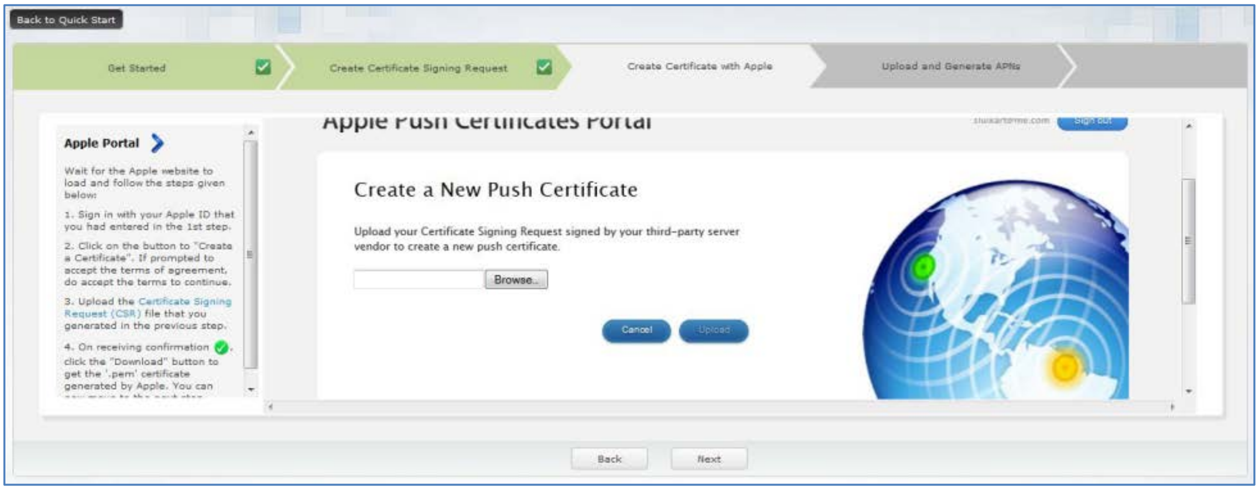
1. Accepting this Agreement; Definitions

1.1 Acceptance

In order to use the MDM Certificates and related services, You must first agree to this License Agreement. If You do not or cannot agree to this License Agreement, You are not permitted to use the MDM Certificates or related services. Do not download or use the MDM Certificates or any related services in that case.

☑ I have read and agree to these terms and conditions.

9. Now you need to find the file so you can upload it. Click **Browse**.


Back to Quick Start
Get Started ☑
Create Certificate Signing Request ☑
Create Certificate with Apple
Upload and Generate APNs
Apple Push Certificates Portal
Sign out
Browse..
Cancel
Upload
Back
Next

Apple Portal

Wait for the Apple website to load and follow the steps given below:

1. Sign in with your Apple ID that you had entered in the 1st step.

2. Click on the button to "Create a Certificate". If prompted to accept the terms of agreement, do accept the terms to continue.

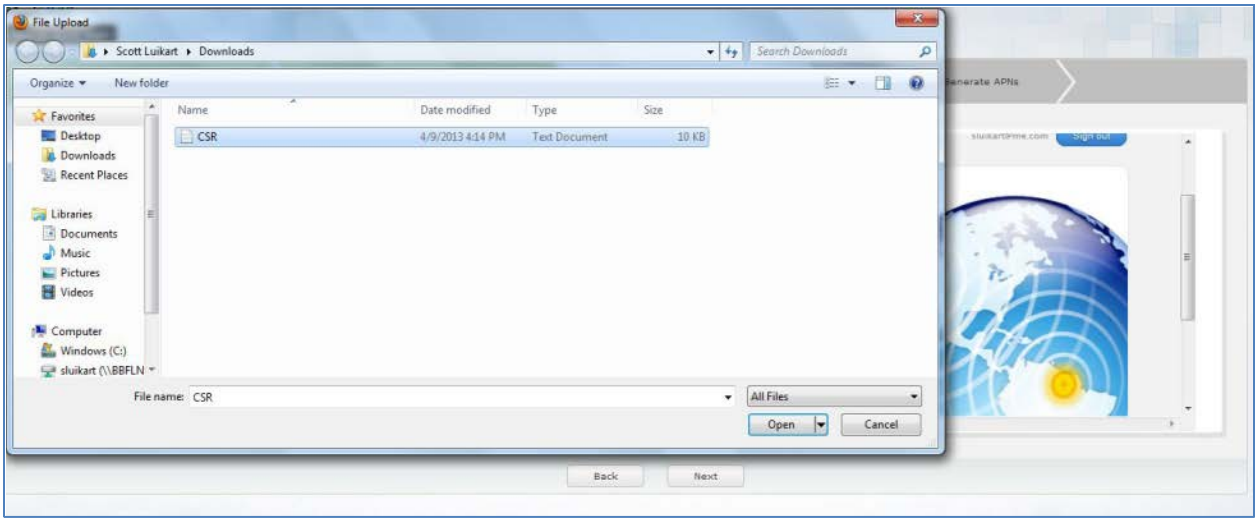
3. Upload the Certificate Signing Request (CSR) file that you generated in the previous step.

4. On receiving confirmation ✓, click the "Download" button to get the '.pem' certificate generated by Apple. You can

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

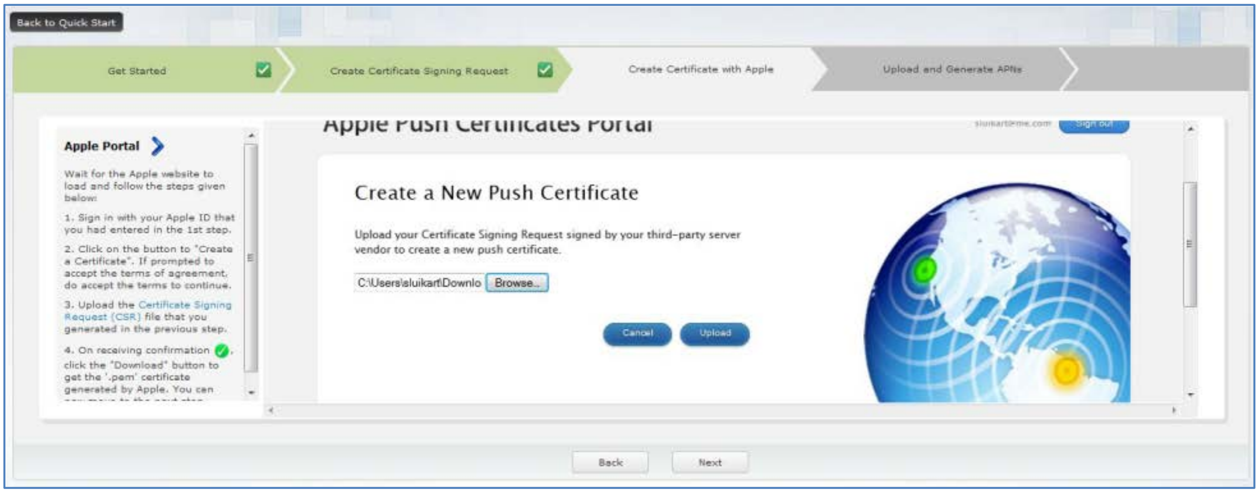
10. Find the CSR.txt file in your **Downloads** folder. Click **Open**.



Name	Date modified	Type	Size
CSR	4/9/2013 4:14 PM	Text Document	10 KB

File name: CSR

11. When the correct file is show in the field, click **Upload**.


Back to Quick Start
Get Started ☑
Create Certificate Signing Request ☑
Create Certificate with Apple
Upload and Generate APNs
Apple Push Certificates Portal
Sign out
Browse...
Cancel
Upload
Back
Next

Apple Portal

Wait for the Apple website to load and follow the steps given below:

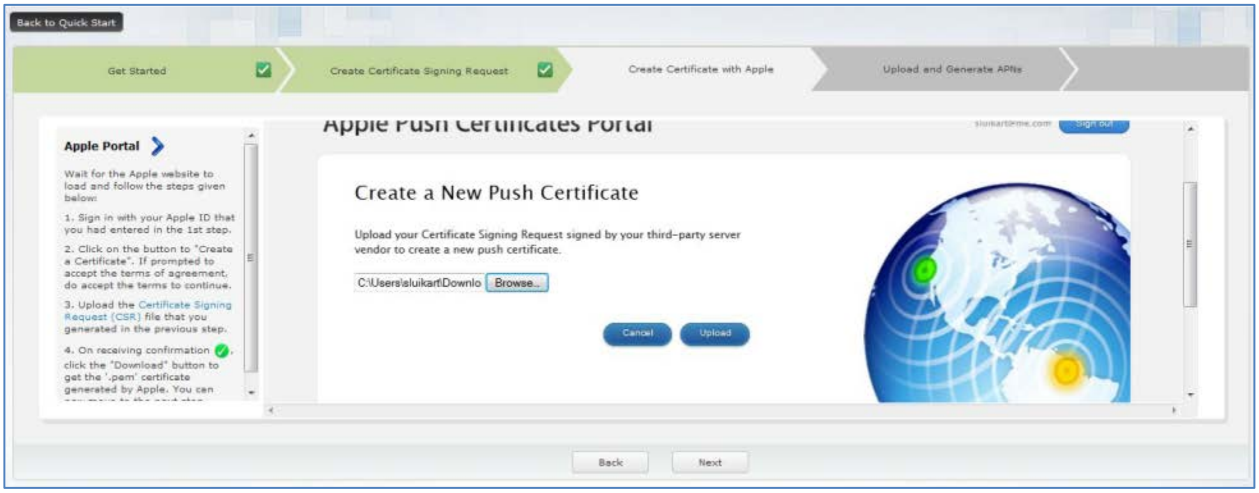
1. Sign in with your Apple ID that you had entered in the 1st step.
2. Click on the button to "Create a Certificate". If prompted to accept the terms of agreement, do accept the terms to continue.
3. Upload the Certificate Signing Request (CSR) file that you generated in the previous step.
4. On receiving confirmation ✓, click the "Download" button to get the '.pem' certificate generated by Apple. You can

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

C:\Users\sluikart\Downlo

12. Click **Download** to download the PEM file. You will also receive this in email just like the CSR.txt file, but you will be using it in the very next step.



Wait for the Apple website to load and follow the steps given below:

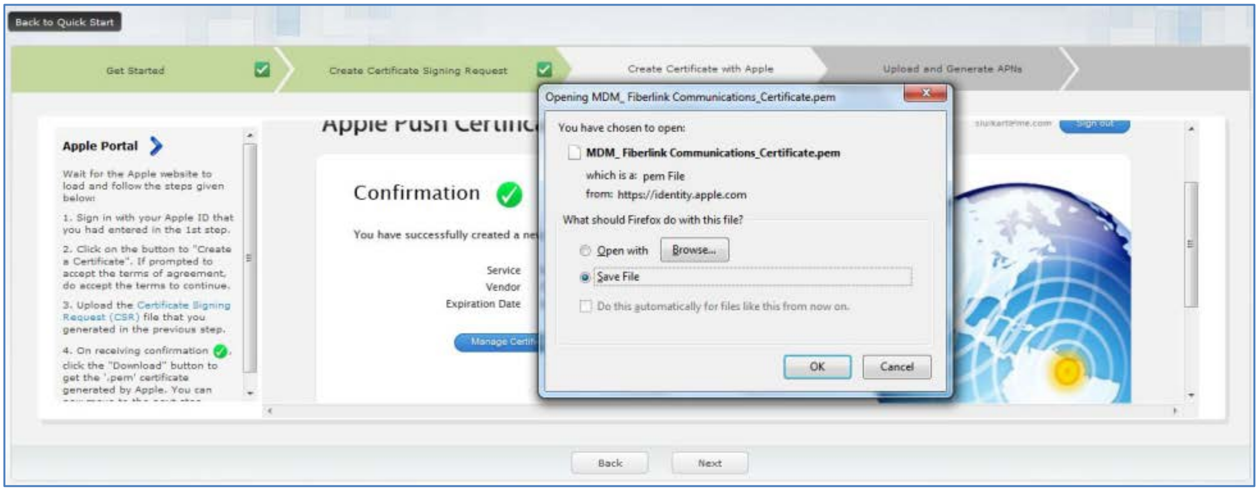
1. Sign in with your Apple ID that you had entered in the 1st step.
2. Click on the button to "Create a Certificate". If prompted to accept the terms of agreement, do accept the terms to continue.
3. Upload the Certificate Signing Request (CSR) file that you generated in the previous step.
4. On receiving confirmation ✓, click the "Download" button to get the '.pem' certificate generated by Apple. You can

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

C:\Users\sluikart\Downlo

13. Click **OK** to save the PEM to your **Downloads** folder.



Confirmation ✓

You have successfully created a ne

Service

Vendor

Expiration Date

Opening MDM_Fiberlink Communications_Certificate.pem

You have chosen to open:

MDM_Fiberlink Communications_Certificate.pem

which is a: pem File

from: https://identity.apple.com

What should Firefox do with this file?

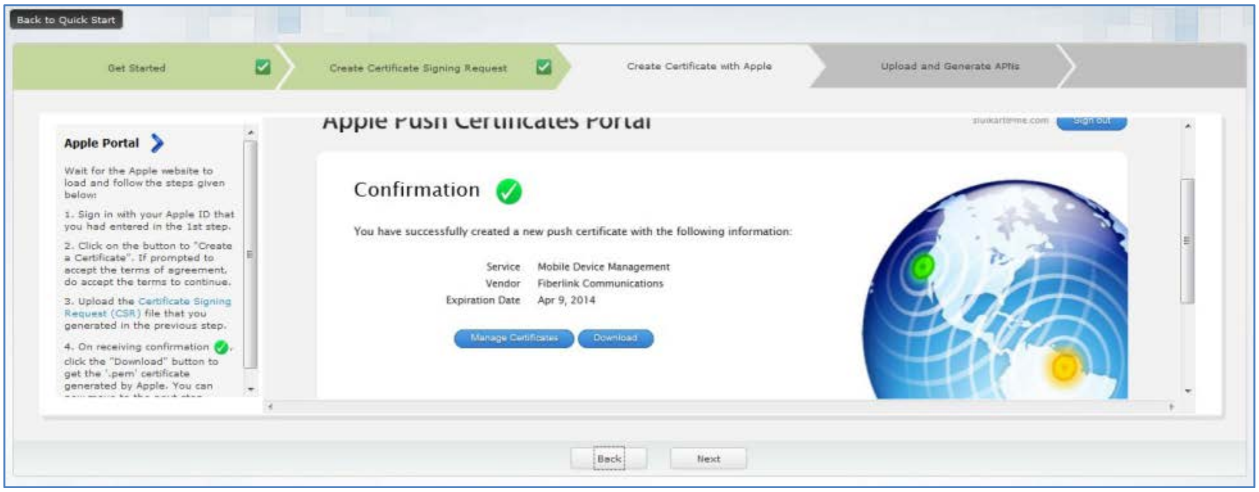
○ Open with Browse...

● Save File

□ Do this automatically for files like this from now on.

OK Cancel

14. You will receive a confirmation message. Click **Next**.

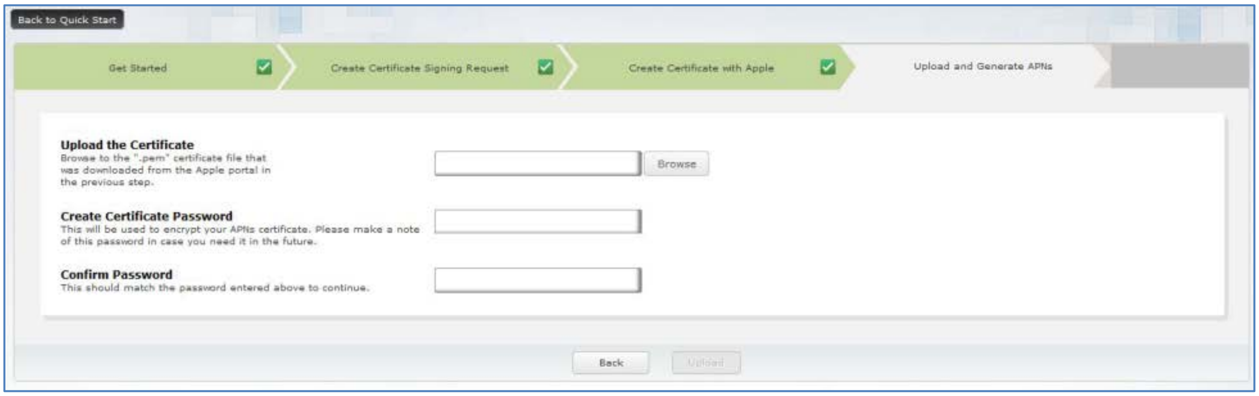


Confirmation ✓

You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	Fiberlink Communications
Expiration Date	Apr 9, 2014

15. Now you have to upload the certificate to MaaS360. Click **Browse**.

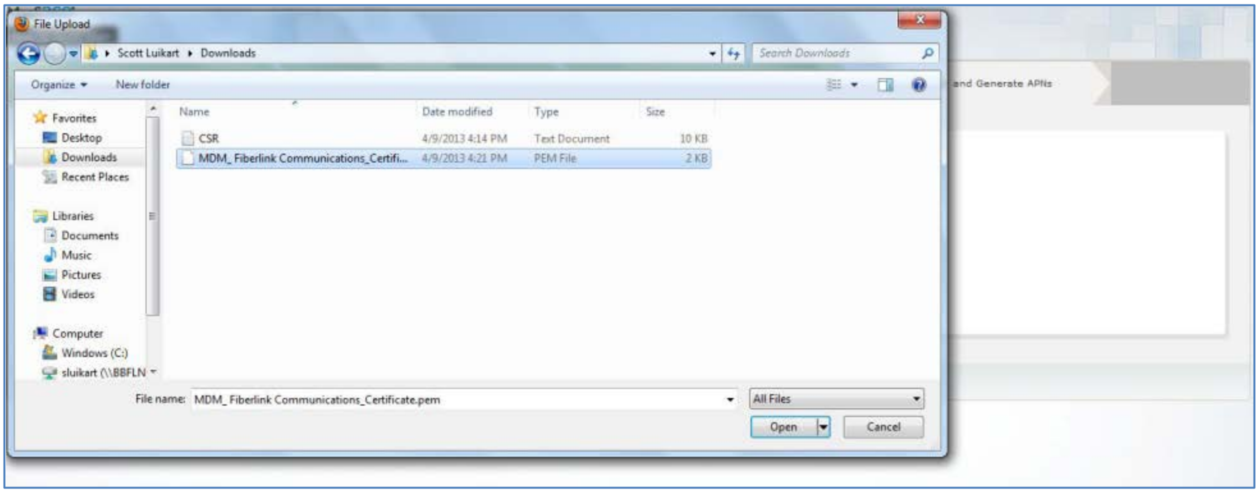


Upload the Certificate
Browse to the ".pem" certificate file that was downloaded from the Apple portal in the previous step.

Create Certificate Password
This will be used to encrypt your APNs certificate. Please make a note of this password in case you need it in the future.

Confirm Password
This should match the password entered above to continue.

16. Find the file MDM_Fiberlink_Communications.pem in your **Downloads** folder. Click **Open**.



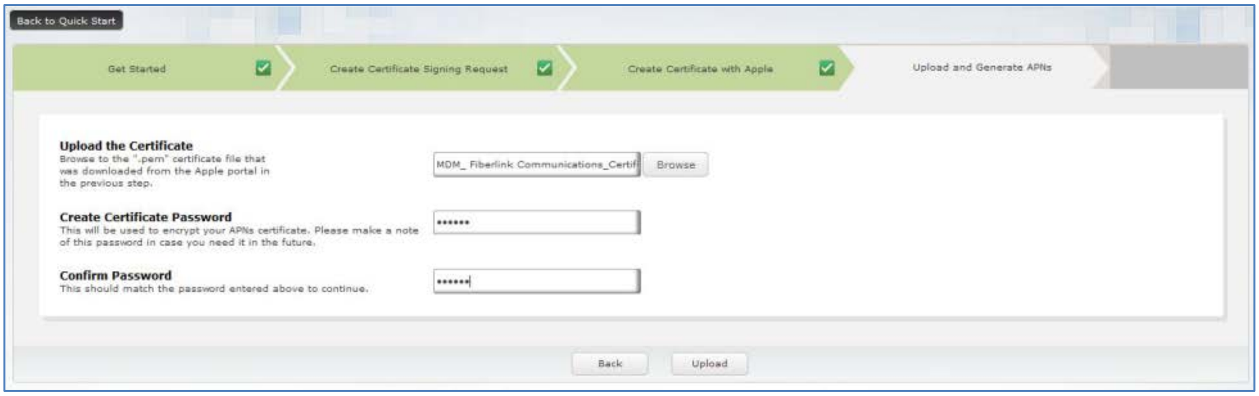
Name	Date modified	Type	Size
CSR	4/9/2013 4:14 PM	Text Document	10 KB
MDM_ Fiberlink Communications_Certifi...	4/9/2013 4:21 PM	PEM File	2 KB

File name: MDM_ Fiberlink Communications_Certificate.pem

All Files

17. Enter a password. This password has no minimum security requirement. To help you remember the password, you may want to make it the same as your AppleID password.

    After entering it in the **Create Certificate Password** and **Confirm Password** fields, click **Upload**.

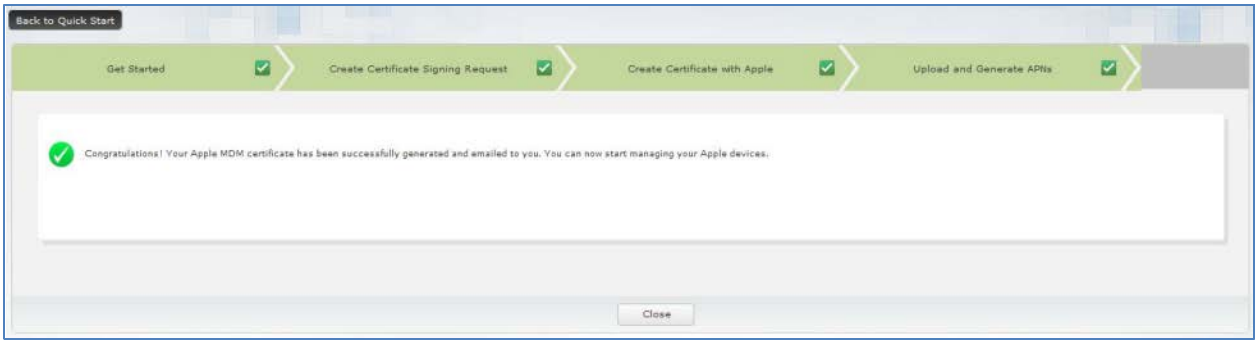


Upload the Certificate
Browse to the ".pem" certificate file that was downloaded from the Apple portal in the previous step.
MDM_ Fiberlink Communications_Certif

Create Certificate Password
This will be used to encrypt your APNs certificate. Please make a note of this password in case you need it in the future.
••••••

Confirm Password
This should match the password entered above to continue.
••••••

18. The APNs certificate has been created. Click **Close**.

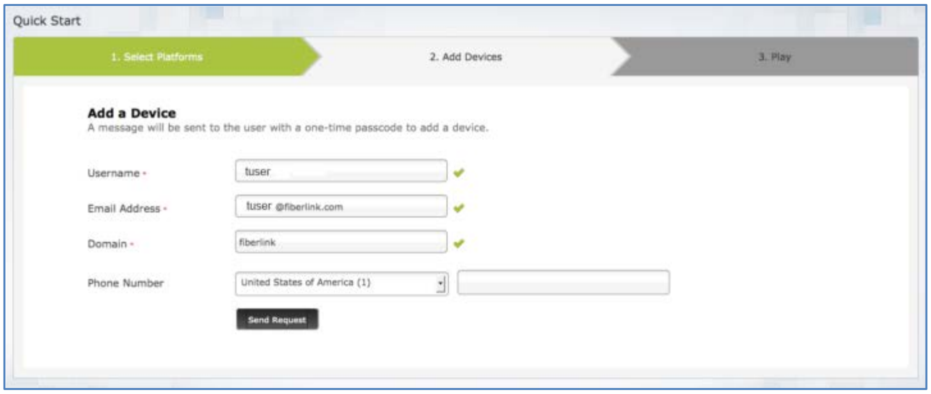

Back to Quick Start
Get Started
Create Certificate Signing Request
Create Certificate with Apple
Upload and Generate APNs
Close

Congratulations! Your Apple MDM certificate has been successfully generated and emailed to you. You can now start managing your Apple devices.

19. MaaS360 will automatically take you to the next step, adding a device.

Step 2: Add Devices

Click the second tab to begin enrolling devices in MaaS360.



Add a Device

A message will be sent to the user with a one-time passcode to add a device.

Username * tuser ✓

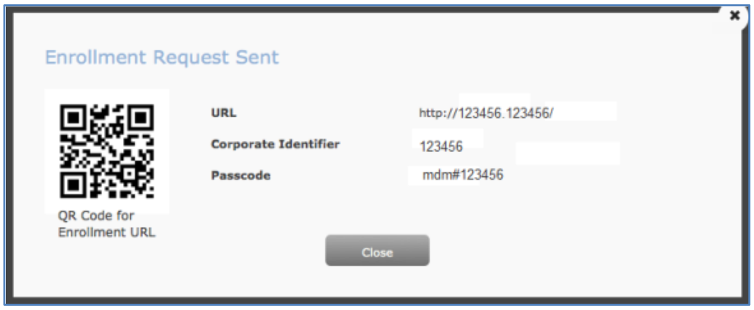
Email Address * tuser @fiberlink.com ✓

Domain * fiberlink ✓

Phone Number United States of America (1)

1. Information from your enrollment will be automatically entered in the **Username**, **Email Address** and **Phone Number** fields, but you can override it. Review the **Domain** field; it is used for email and wireless set up, and more.
2. Click **Send Request**.

   MaaS360 will send an enrollment request to the specified device.



Enrollment Request Sent

URL http://123456.123456/

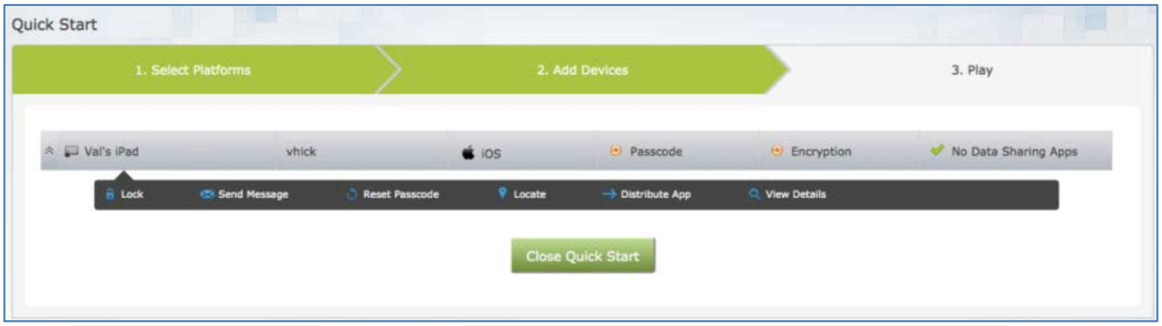
Corporate Identifier 123456

Passcode mdm#123456

When the end user gets the enrollment request, they will be directed to download the MaaS360 app. With just a few taps, they will install the app and the device will begin to send data to MaaS360.

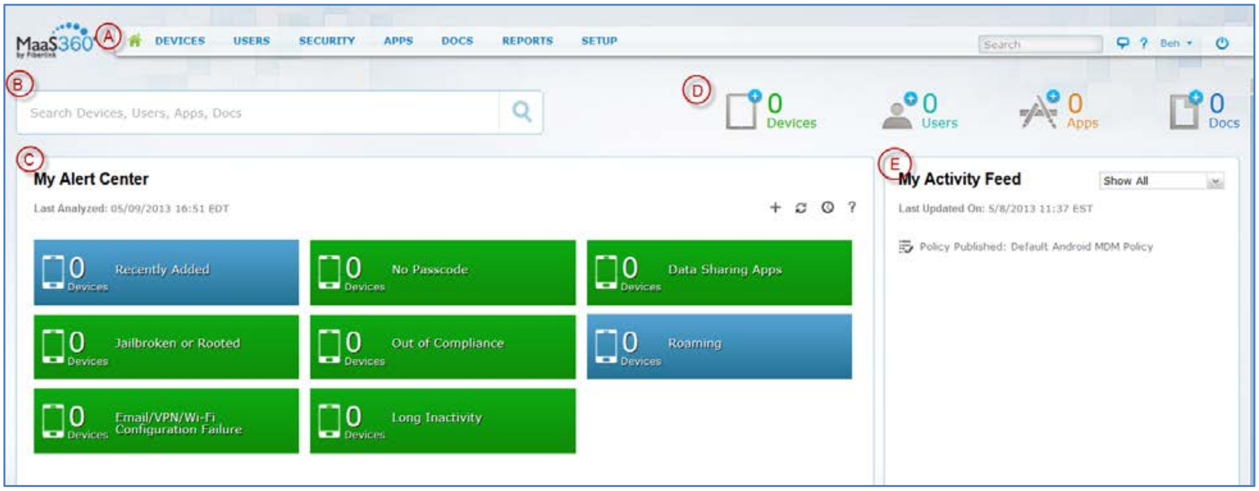
Step 3: Play

Now you can review information about the enrolled device, take actions like Lock, Locate or Distribute App and more.



When you are finished, click **Close Quick Start** to access the MaaS360 **Home** page.

Home Page


MaaS360 by Fiberlink
A
DEVICES
USERS
SECURITY
APPS
DOCS
REPORTS
SETUP
Search
? Ben
B
Search Devices, Users, Apps, Docs
D
0 Devices
0 Users
0 Apps
0 Docs
C
My Alert Center
Last Analyzed: 05/09/2013 16:51 EDT
0 Devices Recently Added
0 Devices No Passcode
0 Devices Data Sharing Apps
0 Devices Jailbroken or Rooted
0 Devices Out of Compliance
0 Devices Roaming
0 Devices Email/VPN/Wi-Fi Configuration Failure
0 Devices Long Inactivity
E
My Activity Feed
Show All
Last Updated On: 5/8/2013 11:37 EST

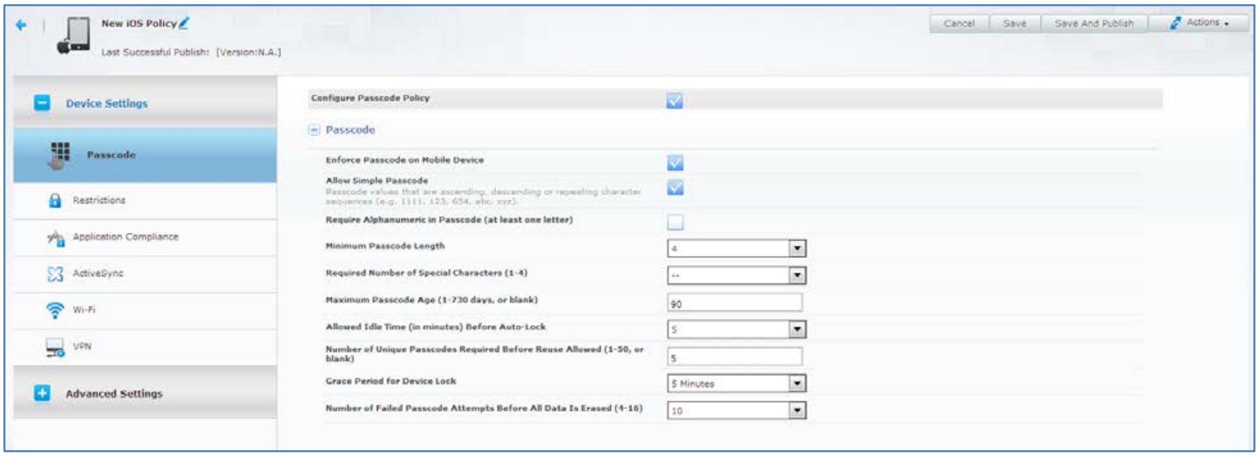
Policy Published: Default Android MDM Policy

A	The menu bar gives you access to different parts of MaaS360. Mouse over one of the tabs to display a menu, and then click on the item you want. Click the 🏠 icon to return to the **Home** page.
B	Start typing in the Search field and MaaS360 will begin displaying items that match the text, including devices, users, apps, and documents. Different links appear under the item, depending on what the item is. For example, clicking the **Locate** link under a device will display it on a map, while clicking the **Distribute** link under an app will allow you to distribute it.
C	My Alert Center draws your attention to important details about your environment. Blue alerts are information only, while red alerts indicate a problem and green ones mean that the situation does not need your attention. You can create and customize these alerts quickly and easily.
D	MaaS360 displays a snapshot of your environment at the top of the screen. The numbers are links to the most commonly used screens in MaaS360, and you can click ⊕ to add a device, user, app or document.
E	My Activity Feed shows you what has been happening in MaaS360. You can filter to see specific types of activities, and click on an item to see details. Compliance events are highlighted.

Security Policies

Policies allow you to enforce your company’s security requirements on mobile devices. Mouse over the **Security** tab at the top of the screen and click **Policies**.

Default policies are included with MaaS360, which you can use as a basis to create custom ones.



New iOS Policy

Last Successful Publish: [Version:N.A.]

Configure Passcode Policy	☑

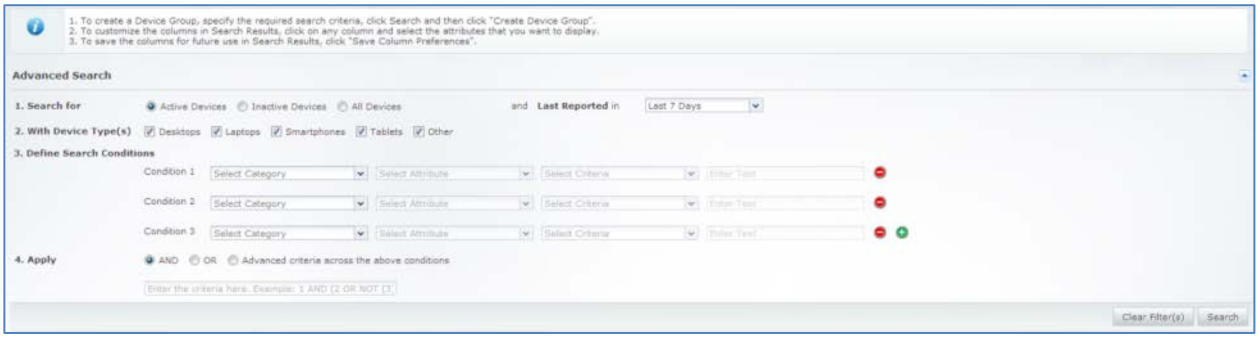
Passcode

Enforce Passcode on Mobile Device	☑
Allow Simple Passcode Passcode values that are ascending, descending or repeating character sequences (e.g. 1111, 123, 654, abc, xyz).	☑
Require Alphanumeric in Passcode (at least one letter)	□
Minimum Passcode Length	4
Required Number of Special Characters (1-4)	--
Maximum Passcode Age (1-730 days, or blank)	90
Allowed Idle Time (in minutes) Before Auto-Lock	5
Number of Unique Passcodes Required Before Reuse Allowed (1-50, or blank)	5
Grace Period for Device Lock	5 Minutes
Number of Failed Passcode Attempts Before All Data Is Erased (4-16)	10

Click the tabs on the left side of the screen to see all the choices. When you have finished, save and publish it. Your policy cannot be deployed to a device until it has been published.

Advanced Search

The **Advanced Search** allows you to perform basic and advanced searches for devices. Select **Devices > Advanced Search**.



1. To create a Device Group, specify the required search criteria, click Search and then click "Create Device Group".
2. To customize the columns in Search Results, click on any column and select the attributes that you want to display.
3. To save the columns for future use in Search Results, click "Save Column Preferences".

Advanced Search

1. Search for ● Active Devices ○ Inactive Devices ○ All Devices and Last Reported in Last 7 Days

2. With Device Type(s) ☑ Desktops ☑ Laptops ☑ Smartphones ☑ Tablets ☑ Other

3. Define Search Conditions

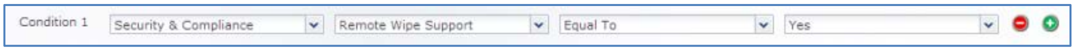
Condition 1 Select Category | Select Attribute | Select Criteria | Enter Text

Condition 2 Select Category | Select Attribute | Select Criteria | Enter Text

Condition 3 Select Category | Select Attribute | Select Criteria | Enter Text

4. Apply ● AND ○ OR ○ Advanced criteria across the above conditions

Enter the criteria here. Example: 1 AND (2 OR NOT (3

Search for	Specify if you want to search for active devices, inactive devices or all devices.
Last Reported	Specify the time period in which the devices last contacted MaaS360.
With Device Type(s)	The options listed here will vary depending on what you have purchased. Specify the device types you want to include in the search.
Define Search Conditions	Specify the category, attribute and value being searched for. For example, to see all the devices that can support remote wipe, enter the following:  Condition 1 Security & Compliance | Remote Wipe Support | Equal To | Yes
Apply	Specify any Boolean operators that should be used to handle multiple search conditions. Enter the additional criteria in the text box.

Click ⊕ to add a row, and click ⊖ to remove one.

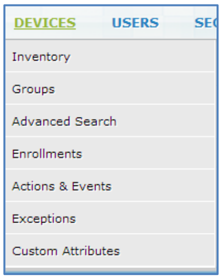
Click **Search** to view results matching the selected criteria. The results will appear in the lower half of the screen.

Your searches can be used for different purposes:

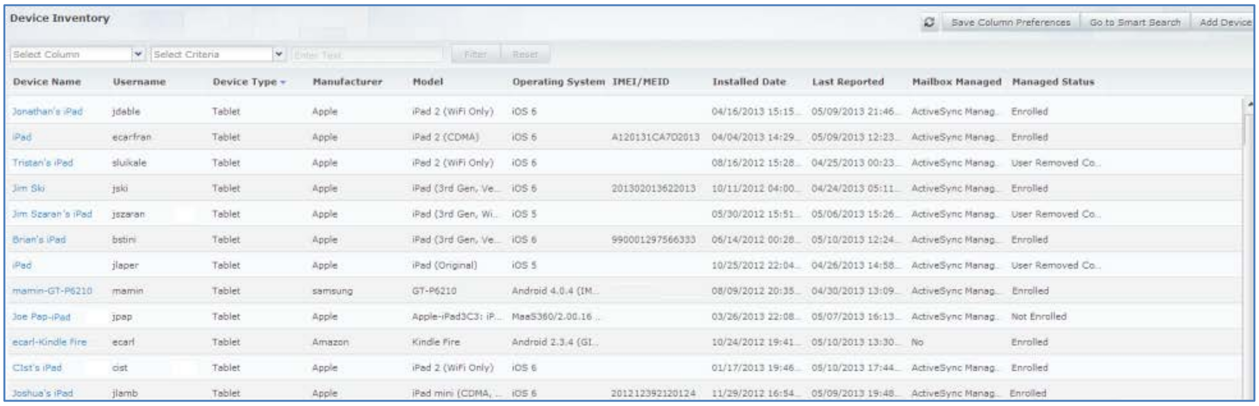
- The alerts on the **Home** page are based on these searches
- You can use these searches to define groups
- You can customize the columns that appear in the results section

Inventory

Select **Devices** > **Inventory** to see the Device Inventory screen, or click the Devices link on the Home page.

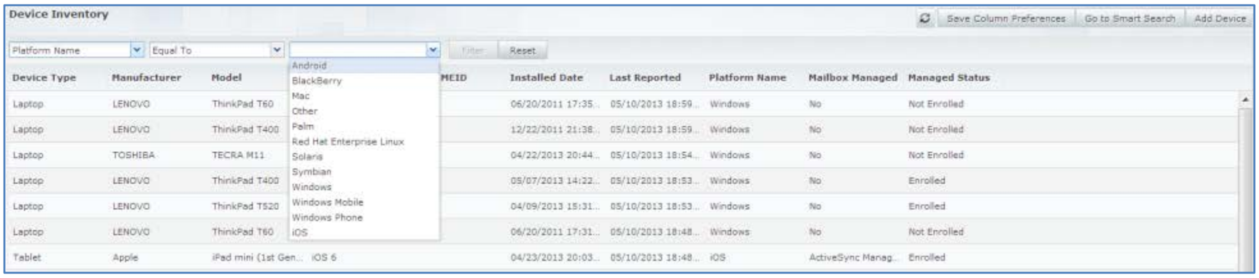


The Device Inventory lists your devices.



Device Name	Username	Device Type	Manufacturer	Model	Operating System	IMEI/MEID	Installed Date	Last Reported	Mailbox Managed	Managed Status
Jonathan's iPad	jdable	Tablet	Apple	iPad 2 (WiFi Only)	iOS 6		04/16/2013 15:15...	05/09/2013 21:46...	ActiveSync Manag...	Enrolled
iPad	ecarfran	Tablet	Apple	iPad 2 (CDMA)	iOS 6	A120131CA7D2013	04/04/2013 14:29...	05/09/2013 12:23...	ActiveSync Manag...	Enrolled
Tristan's iPad	slukale	Tablet	Apple	iPad 2 (WiFi Only)	iOS 6		08/16/2012 15:28...	04/25/2013 00:23...	ActiveSync Manag...	User Removed Co...
Jim Ski	jski	Tablet	Apple	iPad (3rd Gen, Ve...	iOS 6	201302013622013	10/11/2012 04:00...	04/24/2013 05:11...	ActiveSync Manag...	Enrolled
Jim Szaran's iPad	jszaran	Tablet	Apple	iPad (3rd Gen, Wi...	iOS 5		05/30/2012 15:51...	05/06/2013 15:26...	ActiveSync Manag...	User Removed Co...
Brian's iPad	bstini	Tablet	Apple	iPad (3rd Gen, Ve...	iOS 6	990001297566333	06/14/2012 00:28...	05/10/2013 12:24...	ActiveSync Manag...	Enrolled
iPad	jlaper	Tablet	Apple	iPad (Original)	iOS 5		10/25/2012 22:04...	04/26/2013 14:58...	ActiveSync Manag...	User Removed Co...
mamin-GT-P6210	mamin	Tablet	samsung	GT-P6210	Android 4.0.4 (IM...		08/09/2012 20:35...	04/30/2013 13:09...	ActiveSync Manag...	Enrolled
Joe Pap-iPad	jpap	Tablet	Apple	Apple-iPad3C3: iP...	MaaS360/2.00.16 ...		03/26/2013 22:08...	05/07/2013 16:13...	ActiveSync Manag...	Not Enrolled
ecarl-Kindle Fire	ecarl	Tablet	Amazon	Kindle Fire	Android 2.3.4 (GI...		10/24/2012 19:41...	05/10/2013 13:30...	No	Enrolled
CIst's iPad	cist	Tablet	Apple	iPad 2 (WiFi Only)	iOS 6		01/17/2013 19:46...	05/10/2013 17:44...	ActiveSync Manag...	Enrolled
Joshua's iPad	jlamb	Tablet	Apple	iPad mini (CDMA, ...	iOS 6	201212392120124	11/29/2012 16:54...	05/09/2013 19:48...	ActiveSync Manag...	Enrolled

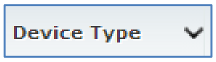
You can use the filter to find specific devices:



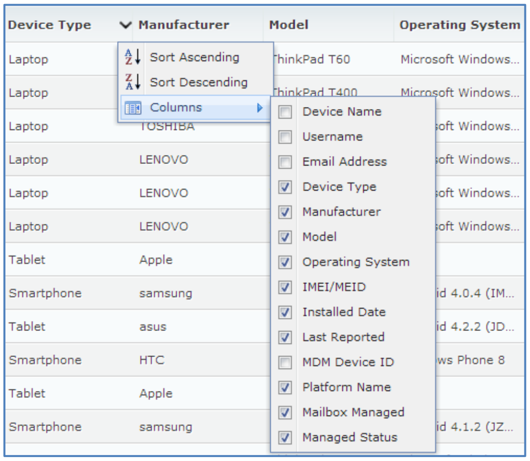
Device Type	Manufacturer	Model		MEID	Installed Date	Last Reported	Platform Name	Mailbox Managed	Managed Status
Laptop	LENOVO	ThinkPad T60			06/20/2011 17:35...	05/10/2013 18:59...	Windows	No	Not Enrolled
Laptop	LENOVO	ThinkPad T400			12/22/2011 21:38...	05/10/2013 18:59...	Windows	No	Not Enrolled
Laptop	TOSHIBA	TECRA M11			04/22/2013 20:44...	05/10/2013 18:54...	Windows	No	Not Enrolled
Laptop	LENOVO	ThinkPad T400			05/07/2013 14:22...	05/10/2013 18:53...	Windows	No	Enrolled
Laptop	LENOVO	ThinkPad T520			04/09/2013 15:31...	05/10/2013 18:53...	Windows	No	Enrolled
Laptop	LENOVO	ThinkPad T60			06/20/2011 17:31...	05/10/2013 18:48...	Windows	No	Not Enrolled
Tablet	Apple	iPad mini (1st Gen...	iOS 6		04/23/2013 20:03...	05/10/2013 18:48...	iOS	ActiveSync Manag...	Enrolled

Click the **Reset** button to remove the filter and see the complete list again.

You can change the columns that are listed by:

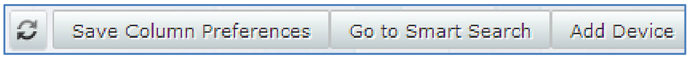
1. Click on the down arrow for a column heading 

2. Select **Columns**, and then check the columns you want to include.



Device Type	Manufacturer	Model	Operating System
Laptop		hinkPad T60	Microsoft Windows...
Laptop		hinkPad T400	Microsoft Windows...
Laptop	TOSHIBA		oft Windows...
Laptop	LENOVO		oft Windows...
Laptop	LENOVO		oft Windows...
Laptop	LENOVO		oft Windows...
Tablet	Apple		
Smartphone	samsung		id 4.0.4 (IM...
Tablet	asus		id 4.2.2 (JD...
Smartphone	HTC		ws Phone 8
Tablet	Apple		
Smartphone	samsung		id 4.1.2 (JZ...

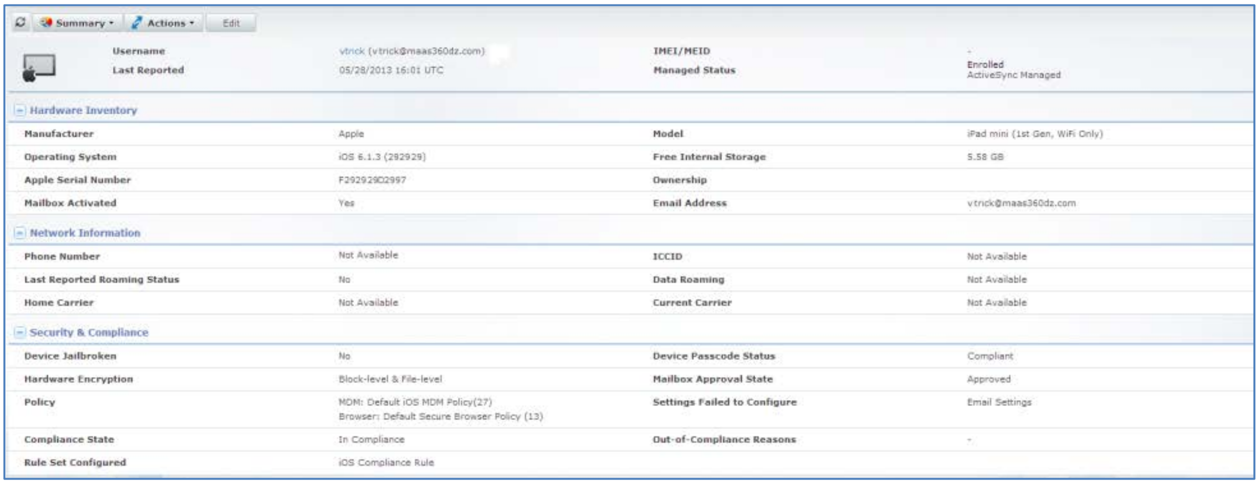
At the top right-hand corner of the screen are additional buttons:



- Click to refresh the information.
- Click **Save Column Preferences** to preserve the changes you made to the columns.
- Click **Go to Advanced Search** to enter advanced search criteria.
- Click **Add Device** to send an enrollment request to a device.

Device Views

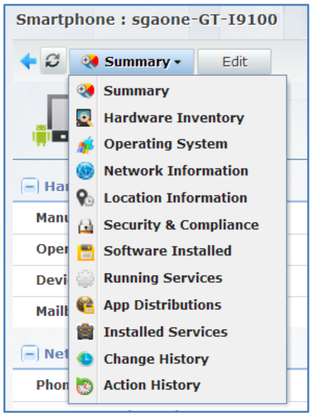
The first device view is the **Summary** screen.



Username	vtrick (vtrick@maas360dz.com)	IMEI/MEID	-
Last Reported	05/28/2013 16:01 UTC	Managed Status	Enrolled ActiveSync Managed
Hardware Inventory			
Manufacturer	Apple	Model	iPad mini (1st Gen, WiFi Only)
Operating System	iOS 6.1.3 (292929)	Free Internal Storage	5.58 GB
Apple Serial Number	F29292902997	Ownership	
Mailbox Activated	Yes	Email Address	vtrick@maas360dz.com
Network Information			
Phone Number	Not Available	ICCID	Not Available
Last Reported Roaming Status	No	Data Roaming	Not Available
Home Carrier	Not Available	Current Carrier	Not Available
Security & Compliance			
Device Jailbroken	No	Device Passcode Status	Compliant
Hardware Encryption	Block-level & File-level	Mailbox Approval State	Approved
Policy	MDM: Default iOS MDM Policy(27) Browser: Default Secure Browser Policy (13)	Settings Failed to Configure	Email Settings
Compliance State	In Compliance	Out-of-Compliance Reasons	-
Rule Set Configured	iOS Compliance Rule		

Click to refresh the information.

Additional screens are available by clicking the pull-down menu. Different screens may be listed depending on the device.

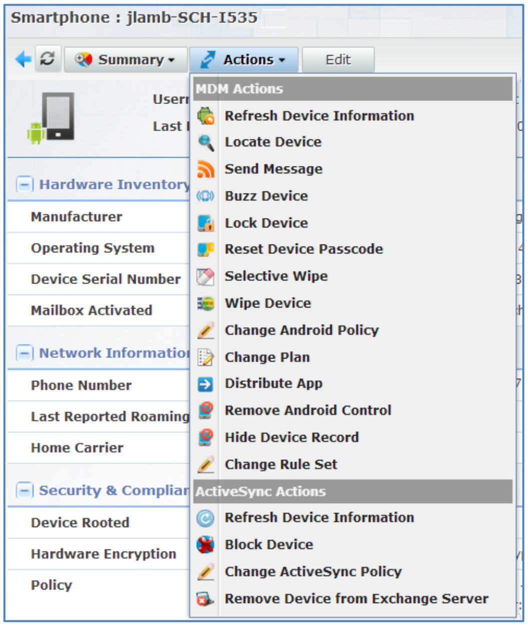


- **Summary**: Basic information about the device, including network and compliance information.
- **Hardware Inventory**: Detailed hardware and storage information about the device. Click **Edit** to update custom attribute information.
- **Operating System**: The OS, OS version, kernel version, API level and more.
- **Network Information**: Detailed information about the cellular network, Wi-Fi network and more.
- **Location Information**: A map showing the last known location of the device.
- **Security & Compliance**: Detailed information about passwords, encryption, the policy, data syncing, and more.
- **Software Installed**: The apps on the device, including the version, size and type.
- **Modules** (appears only if the Cloud Extender is installed for use with the BlackBerry Enterprise Server): The modules on the device, including the version and size.
- **Service Books** (appears only if the Cloud Extender is installed for use with the BlackBerry Enterprise Server): The service books on the device, including the service ID and content ID.
- **Running Services**: The services on the device, including the app ID, memory used, and running time.
- **App Distributions**: The apps that have been distributed to the device by MaaS360; including when they were deployed and which ones have been installed.
- **Installed Services**: Information about the MaaS360 app that is running on the device.
- **Change History**: Information about changes made to the account.
- **Action History**: Lists the actions performed on the device.

Actions

You can perform actions on the device from the Device View.

Note: *The Actions that appear depend on a number of factors, including the device type and how it is being managed, and if the Cloud Extender is installed for ActiveSync options, etc. Refer to Appendix A for details.*



- **Refresh Device Information**: Retrieves the most recent data from the mobile device
- **Last Known Location**: Locates the mobile device
- **Send Message**: Sends a message to it
- **Buzz Device**: Sends an alert tone to help locate it in the immediate area
- **Lock Device**: Sends a command that will lock it
- **Reset Device Passcode**: Clears the current passcode
- **Selective Wipe**: Deletes the Wi-Fi profile, Exchange ActiveSync profiles, and Web shortcuts configured on the device via MaaS360 policy. It can also remove apps and documents, if the appropriate options were selected when they were loaded into the App Catalog and Content Library, respectively
- **Wipe Device**: Erases all data on the device and resets it to the original factory settings. For Android 2.2, the Wipe Device action will reset only the phone memory. However, in Android 2.3, it will reset both the phone memory and the SD card
- **Change iOS/Android Policy**: Allows you to change the policy in force on the device
- **Change Plan**: Allows you to change the Mobile Expense Management plan
- **Distribute App**: Distribute an app to the device
- **Remove Control**: Allows you to unregister the device from MaaS360, and MaaS360 cannot manage it anymore. The first part of the process is a selective wipe of the device
- **Hide Device Record**: Marks a device as inactive in MaaS360 reporting, but it does not remove control on the device. This should only be performed if the device is permanently offline, destroyed, etc.
- **Change Rule Set**: Allows you to apply or update the rule set assigned to a device
- **Refresh Device Information (EAS)**: Refreshes the information shown for the device from Exchange ActiveSync
- **Block Device (EAS)**: Prevents the device from accessing your Exchange ActiveSync server

- **Change ActiveSync Policy (EAS)**: Changes the policy in force on the device. These settings will be specific to Exchange ActiveSync
- **Remove Device from Exchange Server (EAS)**: Removes the device records from your Exchange ActiveSync server
- **Reset Device Passcode (BlackBerry)**: Clears the current passcode
- **Wipe Device (BlackBerry)**: Allows you to wipe data and settings deployed from MaaS360
- **Change BES Policy (BlackBerry)**: Changes the policy in force on the device
- **Remove Device from BES (BlackBerry)**: Removes the device records from your BES server
- **Block Device (Lotus Traveler)**: Prevents the device from accessing your Lotus Traveler server
- **Wipe Device (Lotus Traveler)**: Allows you to wipe data and settings deployed from MaaS360
- **Remove Device from Traveler (Lotus Traveler)**: Removes the device records from your Lotus Traveler server
- **Change Rule Set (Lotus Traveler)**: Allows you to apply or update the rule set assigned to a device
- **Hide Device Record (Lotus Traveler)**: Marks a device as inactive in MaaS360 reporting, but it does not remove control on the device. This should only be performed if the device is permanently offline, destroyed, etc.

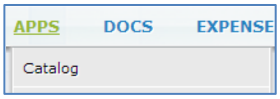
Applications

The app management features of MaaS360 are accessed from the **Apps** tab.

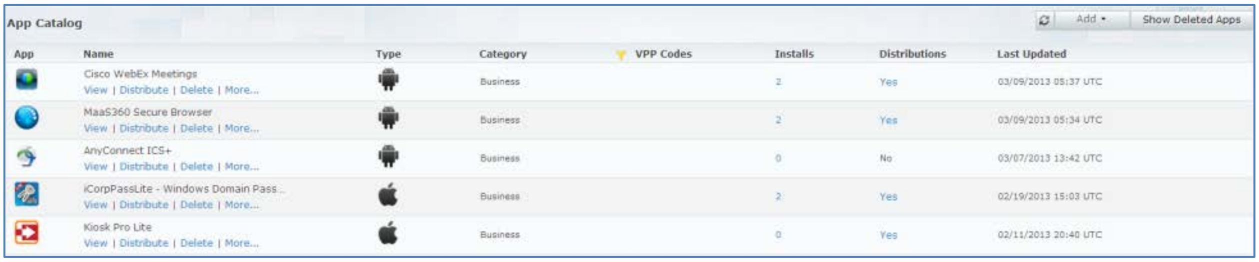
The App Catalog

MaaS360 allows you to deploy apps to your users quickly and easily. Each app must be loaded into the MaaS360 App Catalog before it can be distributed.

To access the App Catalog, mouse over **Apps** and click **Catalog**.



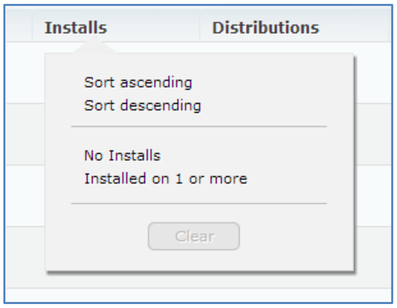
The App Catalog lists your apps and provides basic information about them.



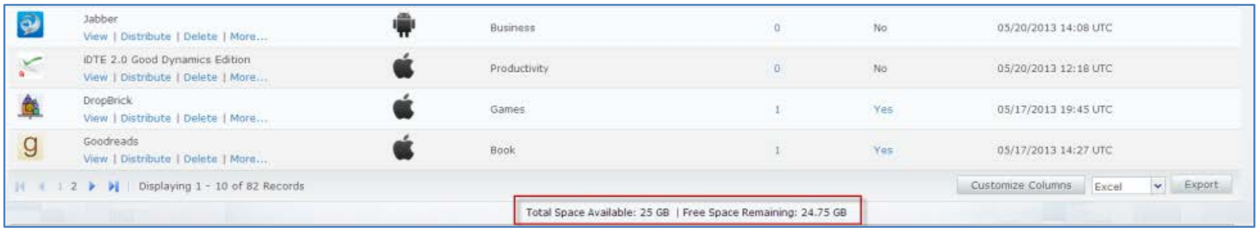
App Catalog

App	Name	Type	Category	VPP Codes	Installs	Distributions	Last Updated
	Cisco WebEx Meetings View | Distribute | Delete | More...		Business		2	Yes	03/09/2013 05:37 UTC
	MaaS360 Secure Browser View | Distribute | Delete | More...		Business		2	Yes	03/09/2013 05:34 UTC
	AnyConnect ICS+ View | Distribute | Delete | More...		Business		0	No	03/07/2013 13:42 UTC
	iCorpPassLite - Windows Domain Pass... View | Distribute | Delete | More...		Business		2	Yes	02/19/2013 15:03 UTC
	Kiosk Pro Lite View | Distribute | Delete | More...		Business		0	Yes	02/11/2013 20:40 UTC

You can sort and filter your apps by clicking on the column headings.



At the bottom of the screen you can see how much storage you are using, and how much is available.



	Jabber View | Distribute | Delete | More...		Business	0	No	05/20/2013 14:08 UTC
	iDTE 2.0 Good Dynamics Edition View | Distribute | Delete | More...		Productivity	0	No	05/20/2013 12:18 UTC
	DropBrick View | Distribute | Delete | More...		Games	1	Yes	05/17/2013 19:45 UTC
	Goodreads View | Distribute | Delete | More...		Book	1	Yes	05/17/2013 14:27 UTC

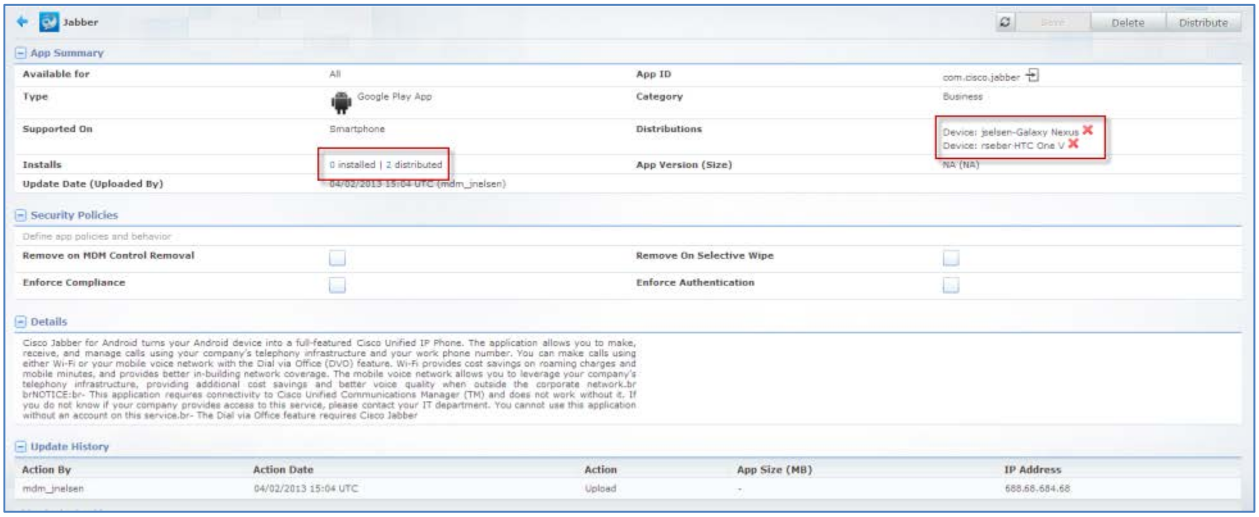
1 2 | Displaying 1 - 10 of 82 Records

Total Space Available: 25 GB | Free Space Remaining: 24.75 GB

There are links under each app you can use to take action.

View

Click the **View** link to see detailed information about the app.



App Summary

Available for	All	App ID	com.cisco.jabber
Type	Google Play App	Category	Business
Supported On	Smartphone	Distributions	Device: jselsen-Galaxy Nexus ✖ Device: rseber-HTC One V ✖
Installs	0 installed | 2 distributed	App Version (Size)	NA (NA)
Update Date (Uploaded By)	04/02/2013 15:04 UTC (mdm_jnelsen)		

Security Policies

Define app policies and behavior

Remove on MDM Control Removal	□	Remove On Selective Wipe	□
Enforce Compliance	□	Enforce Authentication	□

Details

Cisco Jabber for Android turns your Android device into a full-featured Cisco Unified IP Phone. The application allows you to make, receive, and manage calls using your company's telephony infrastructure and your work phone number. You can make calls using either Wi-Fi or your mobile voice network with the Dial via Office (DVO) feature. Wi-Fi provides cost savings on roaming charges and mobile minutes, and provides better in-building network coverage. The mobile voice network allows you to leverage your company's telephony infrastructure, providing additional cost savings and better voice quality when outside the corporate network.br brNOTICE:br- This application requires connectivity to Cisco Unified Communications Manager (TM) and does not work without it. If you do not know if your company provides access to this service, please contact your IT department. You cannot use this application without an account on this service.br- The Dial via Office feature requires Cisco Jabber

Update History

Action By	Action Date	Action	App Size (MB)	IP Address
mdm_jnelsen	04/02/2013 15:04 UTC	Upload	-	688.68.684.68

You can see:

- The type of app
- The category
- How many devices it was distributed to
- How many have installed it
- Any security policies in effect for it
- An audit trail

If there are pending distributions, they will be marked with a red **X**. You can click the **X** to cancel the specified distribution.

Distribute

Click the **Distribute** link to choose the options you want for distributing the app. There are different options depending on the type of app.

Different options are displayed depending on the type of app:

- iTunes App Store App:
    - **Available for**: Specify who can receive the app, either all users or a group
    - **Target**: Specify if it will be deployed to a device, a group or a specific device
    - **Instant Install (iOS 5+ devices)**: Recipients will be prompted to install the app (not available for paid apps, unless you are using VPP codes)
    - **Send Email**: Recipients will receive an email telling them that the app has been added to their app catalog
- Enterprise App for iOS:
    - **Available for**: Specify who can receive the app, either all users or a group
    - **Target**: Specify if it will be deployed to a device, a group or a specific device
    - **Instant Install (iOS 5+ devices)**: Recipients will be prompted to install the app (not available for paid apps, unless you are using VPP codes)

    - **Send Email**: Recipients will receive an email telling them that the app has been added to their app catalog

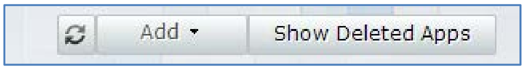
- Google Play App:
    - **Available for**: Specify who can receive the app, either all users or a group
    - **Target**: Specify if it will be deployed to a device, a group or a specific device
    - **Send Email**: Recipients will receive an email telling them that the app has been added to their app catalog
- Enterprise App for Android:
    - **Available for**: Specify who can receive the app, either all users or a group
    - **Target**: Specify if it will be deployed to a device, a group or a specific device
    - **Instant Install**: Specify if the user will be prompted to install the app and the type of network:
        - All Networks
        - Wi-Fi only
        - Wi-Fi and in-network cellular

      Note: *Instant Install is silent for Samsung SAFE devices.*
    - **Send Email**: Recipients will receive an email telling them that the app has been added to their app catalog
- Windows Phone Store App: Send Email
    - **Available for**: Specify who can receive the app, either all users or a group
    - **Target**: Specify if it will be deployed to a device, a group or a specific device
    - **Send Email**: Recipients will receive an email telling them that the app has been added to their app catalog
- Windows Phone Private App:
    - **Target**: Specify if it will be deployed to a device, a group or a specific device
    - **Send Email**: Recipients will receive an email telling them that the app has been added to their app catalog
- Web App for iOS:
    - **Available for**: Specify who can receive the app, either all users or a group
    - **Target**: Specify if it will be deployed to a device, a group or a specific device

Delete

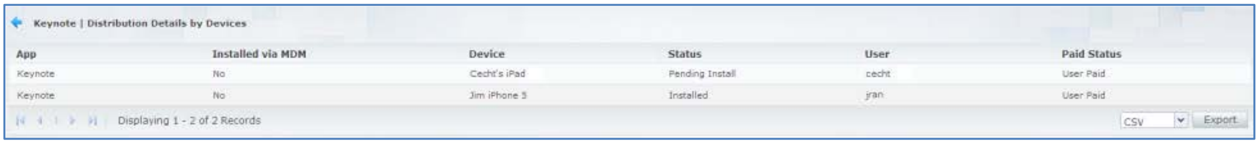
Click the **Delete** link to delete the app from the App Catalog. It cannot be distributed to anyone if it has been deleted.

Click Show Deleted Apps to see all the apps that were deleted. You can only view them.



Distribution Details by Devices

Click the **More** link, and then click **Distribution Details by Devices** to see information about previous distributions.



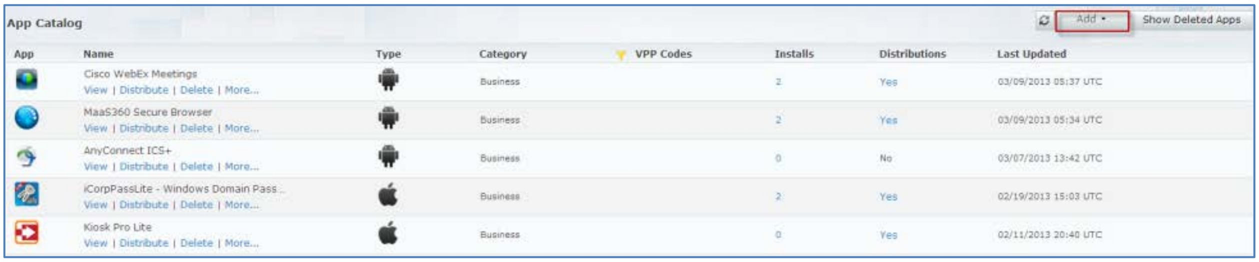
Keynote | Distribution Details by Devices

App	Installed via MDM	Device	Status	User	Paid Status
Keynote	No	Cecht's iPad	Pending Install	cecht	User Paid
Keynote	No	Jim iPhone 5	Installed	jran	User Paid

Displaying 1 - 2 of 2 Records

Adding an App to the App Catalog

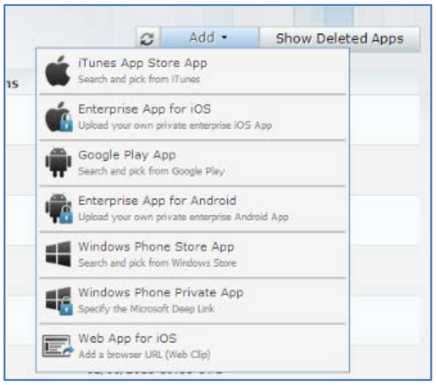
1. Click the **Add** button to add an app.



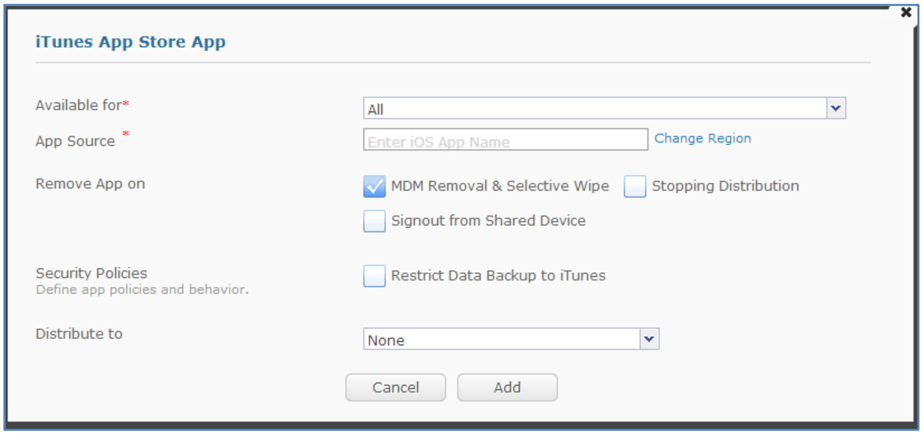
App Catalog

App	Name	Type	Category	VPP Codes	Installs	Distributions	Last Updated
	Cisco WebEx Meetings View | Distribute | Delete | More...		Business		2	Yes	03/09/2013 05:37 UTC
	MaaS360 Secure Browser View | Distribute | Delete | More...		Business		2	Yes	03/09/2013 05:34 UTC
	AnyConnect ICS+ View | Distribute | Delete | More...		Business		0	No	03/07/2013 13:42 UTC
	iCorpPassLite - Windows Domain Pass... View | Distribute | Delete | More...		Business		2	Yes	02/19/2013 15:03 UTC
	Kiosk Pro Lite View | Distribute | Delete | More...		Business		0	Yes	02/11/2013 20:40 UTC

It expands so you can indicate the type of app.


Add ▾
Show Deleted Apps
iTunes App Store App
Search and pick from iTunes
Enterprise App for iOS
Upload your own private enterprise iOS App
Google Play App
Search and pick from Google Play
Enterprise App for Android
Upload your own private enterprise Android App
Windows Phone Store App
Search and pick from Windows Store
Windows Phone Private App
Specify the Microsoft Deep Link
Web App for iOS
Add a browser URL (Web Clip)

2. Specify if the app will be available to all users or a specific group, even if you do not plan to distribute the app to them right away.



iTunes App Store App

Available for* All

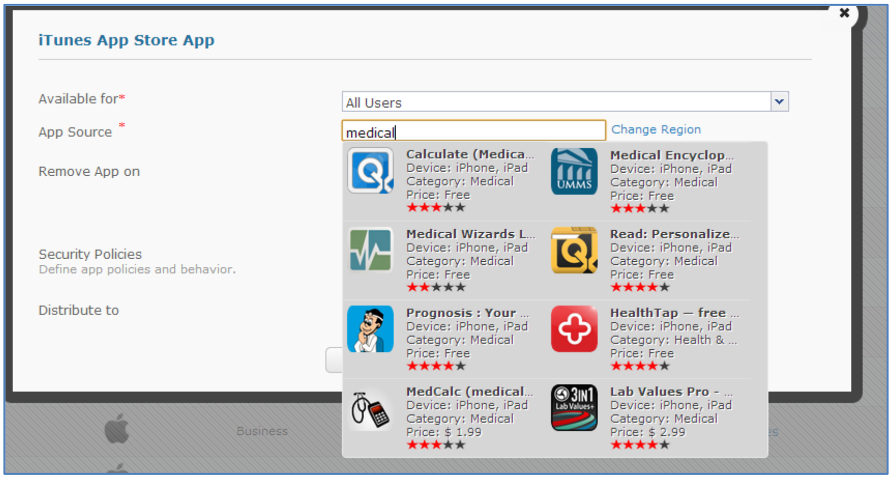
App Source * Enter iOS App Name Change Region

Remove App on ☑ MDM Removal & Selective Wipe ☐ Stopping Distribution ☐ Signout from Shared Device

Security Policies
Define app policies and behavior. ☐ Restrict Data Backup to iTunes

Distribute to None

3. Begin entering the name of the app. MaaS360 will present you with choices as you type.



iTunes App Store App

Available for* All Users

App Source * medical Change Region

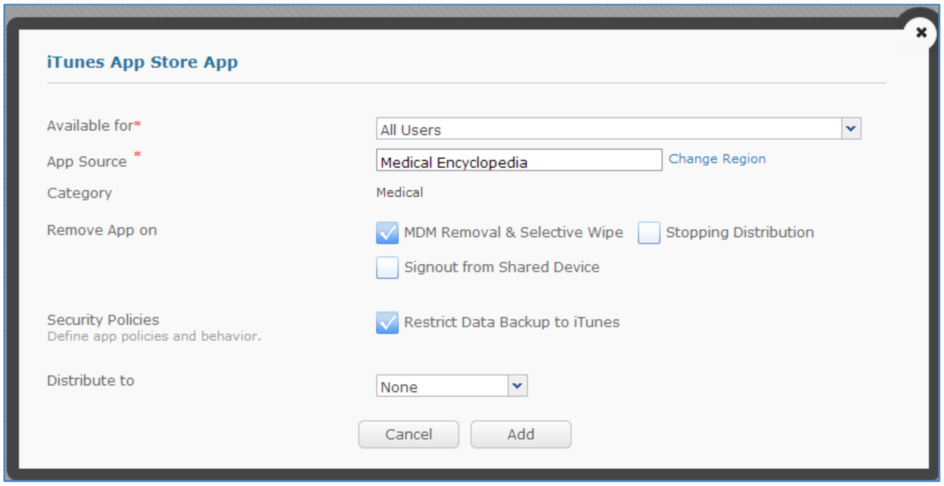
Remove App on

Security Policies
Define app policies and behavior.

Distribute to

Calculate (Medica... Device: iPhone, iPad Category: Medical Price: Free ★★★☆☆	Medical Encyclop... Device: iPhone, iPad Category: Medical Price: Free ★★★☆☆
Medical Wizards L... Device: iPhone, iPad Category: Medical Price: Free ★★☆☆☆	Read: Personalize... Device: iPhone, iPad Category: Medical Price: Free ★★★★☆
Prognosis : Your ... Device: iPhone, iPad Category: Medical Price: Free ★★★★☆	HealthTap — free ... Device: iPhone, iPad Category: Health & ... Price: Free ★★★★☆
MedCalc (medical... Device: iPhone, iPad Category: Medical Price: $ 1.99 ★★★☆☆	Lab Values Pro - ... Device: iPhone, iPad Category: Medical Price: $ 2.99 ★★★★☆

4. Specify the app removal, security and distribution options.



iTunes App Store App

Available for* All Users

App Source * Medical Encyclopedia Change Region

Category Medical

Remove App on ☑ MDM Removal & Selective Wipe ☐ Stopping Distribution
☐ Signout from Shared Device

Security Policies
Define app policies and behavior. ☑ Restrict Data Backup to iTunes

Distribute to None

Different options are displayed depending on the type of app:

- iTunes App Store App:
    - **App Source**: Enter the app's name. Click **Change Region** if need to change the name of the country
    - **Remove App on**
        - **MDM Removal & Selective Wipe**: The app will be removed if MaaS360's control of the device is terminated, or if a selective wipe is performed on the device
        - **Stopping Distribution**: The app will be removed if a pending distribution is ended
    - **Security Policies**
        - **Restrict Data Backup to iTunes:** App data will not be backed up to iTunes
    - **Distribute to**
        - **None**: Load the app into the App Catalog without distributing it
        - **Specific Device**: Enter the device name and specify:
            - **Instant Install**: MaaS360 will prompt the recipient to download the app

            - **Send Email**: MaaS360 will send them an email telling them about the new app
        - **Group:** Select the group of devices to receive the app and specify:
            - **Instant Install**: MaaS360 will prompt the recipient to download the app
            - **Send Email**: MaaS360 will send them an email telling them about the new app
        - **All Devices:** All your devices will receive the app. Specify:
            - **Instant Install**: MaaS360 will prompt the recipient to download the app
            - **Send Email**: MaaS360 will send them an email telling them about the new app

- Enterprise App for iOS:
    - **App Source**: Enter the app's name
    - **Description**: Enter a description of the app
    - **Category**: Enter a classification for the app
    - **Screenshot**: Upload screenshots for the app
    - **Remove App on**
        - **MDM Removal & Selective Wipe**: The app will be removed if MaaS360's control of the device is terminated, or if a selective wipe is performed on the device
        - **Stopping Distribution**: The app will be removed if a pending distribution is ended
    - **Security Policies**
        - **Restrict Data Backup to iTunes:** App data will not be backed up to iTunes
    - **Distribute to**
        - None: Load the app into the App Catalog without distributing it
        - Specific Device: Enter the device name and specify:
            - **Instant Install**: MaaS360 will prompt the recipient to download the app
            - **Send Email**: MaaS360 will send them an email telling them about the new app
        - **Group:** Select the group of devices to receive the app and specify:
            - **Instant Install**: MaaS360 will prompt the recipient to download the app
            - **Send Email**: MaaS360 will send them an email telling them about the new app
        - **All Devices:** All your devices will receive the app. Specify:
            - **Instant Install**: MaaS360 will prompt the recipient to download the app
            - **Send Email**: MaaS360 will send them an email telling them about the new app
- Google Play App:
    - **App Name**: Enter the app's name. Click **Provide URL** if you need to find the app in the Google Play store

- **Remove App on**
  - **MDM Control Removal**: The app will be removed if MaaS360's control of the device is terminated
  - **Selective Wipe**: The app will be removed if a selective wipe is performed on the device
- **Security Policies**
  - **Enforce Authentication:** Users must enter a username and password to receive the app
  - **Enforce Compliance:** Devices must be in compliance to receive the app
- **Distribute to**
  - None: Load the app into the App Catalog without distributing it
  - Specific Device: Enter the device name and specify:
    - **Instant Install**: MaaS360 will prompt the recipient to download the app
    - **Send Email**: MaaS360 will send them an email telling them about the new app
  - **Group:** Select the group of devices to receive the app and specify:
    - **Instant Install**: MaaS360 will prompt the recipient to download the app. Instant Install is silent on Samsung SAFE devices
    - **Send Email**: MaaS360 will send them an email telling them about the new app
  - **All Devices:** All your devices will receive the app. Specify:
    - **Instant Install**: MaaS360 will prompt the recipient to download the app
    - **Send Email**: MaaS360 will send them an email telling them about the new app

- Enterprise App for Android:
  - **App Source**: Upload the file. Click **Provide URL** to use a URL instead
  - **Description**: Enter a description of the app
  - **Category**: Enter a classification for the app
  - **Screenshot**: Upload screenshots for the app
  - **Remove App on**
    - **MDM Control Removal:** The app will be removed if MaaS360's control of the device is terminated
    - **Selective Wipe**: The app will be removed if a selective wipe is performed on the device
  - **Security Policies**
    - **Restrict Data Backup to iTunes:** App data will not be backed up to iTunes
  - **Distribute to**
    - None: Load the app into the App Catalog without distributing it

- Specific Device: Enter the device name and specify:
  - **Instant Install**: MaaS360 will prompt the recipient to download the app. Instant Install is silent on Samsung SAFE devices
  - **Send Email**: MaaS360 will send them an email telling them about the new app
- **Group:** Select the group of devices to receive the app and specify:
  - **Instant Install**: MaaS360 will prompt the recipient to download the app. Instant Install is silent on Samsung SAFE devices
  - **Send Email**: MaaS360 will send them an email telling them about the new app
- **All Devices:** All your devices will receive the app. Specify:
  - **Instant Install**: MaaS360 will prompt the recipient to download the app. Instant Install is silent on Samsung SAFE devices
- **Send Email**: Recipients will receive an email telling them that the app has been added to their app catalog

- Windows Phone Store App:
  - **Windows Phone Store App**: Upload the file. Click **Provide URL** to use a URL instead
  - **Distribute to**
    - None: Load the app into the App Catalog without distributing it
    - Specific Device: Enter the device name and specify:
      - **Instant Install**: MaaS360 will prompt the recipient to download the app
      - **Send Email**: MaaS360 will send them an email telling them about the new app
    - **Group:** Select the group of devices to receive the app and specify:
      - **Instant Install**: MaaS360 will prompt the recipient to download the app
      - **Send Email**: MaaS360 will send them an email telling them about the new app
    - **All Devices:** All your devices will receive the app. Specify:
      - **Instant Install**: MaaS360 will prompt the recipient to download the app
    - **Send Email**: Recipients will receive an email telling them that the app has been added to their app catalog
- Windows Phone Private App:
  - **Windows Phone URL for App**: Specify the URL of the app
  - **Distribute to**
    - None: Load the app into the App Catalog without distributing it
    - Specific Device: Enter the device name and specify:
      - **Instant Install**: MaaS360 will prompt the recipient to download the app

- **Send Email**: MaaS360 will send them an email telling them about the new app

- **Group:** Select the group of devices to receive the app and specify:
  - **Instant Install**: MaaS360 will prompt the recipient to download the app
  - **Send Email**: MaaS360 will send them an email telling them about the new app
- **All Devices:** All your devices will receive the app. Specify:
  - **Instant Install**: MaaS360 will prompt the recipient to download the app
- **Send Email**: Recipients will receive an email telling them that the app has been added to their app catalog

- Web App for iOS:
  - **Web App Display Name**: Enter the app's name
  - **Web App URL:** Enter the complete URL for the app
  - **Web App Icon:** Specify the icon you want to represent the app
  - **Description**: Enter a description of the app
  - **Category**: Enter a classification for the app
  - **Remove App on**
    - **Stopping Distribution**: The app will be removed if a pending distribution is ended

    Note: *iOS Web Apps are always removed if MaaS360's control of the device is terminated or if a selective wipe is performed on it.*
  - **Policies**
    - **Install Automatically:** App data will not be backed up to iTunes
    - **Launch in Full Screen:** Launch the app in full screen mode on the device
    - **Visual Effects on Icon:** The icon will be displayed with standard graphics
    - **Allow Users to Remove:** Allow users to remove the app from the device
  - **Distribute to**
    - None: Load the app into the App Catalog without distributing it
    - Specific Device: Enter the device name and specify:
      - **Instant Install**: MaaS360 will prompt the recipient to download the app
      - **Send Email**: MaaS360 will send them an email telling them about the new app
    - **Group:** Select the group of devices to receive the app and specify:
      - **Instant Install**: MaaS360 will prompt the recipient to download the app
      - **Send Email**: MaaS360 will send them an email telling them about the new app
    - **All Devices:** All your devices will receive the app. Specify:
      - **Instant Install**: MaaS360 will prompt the recipient to download the app

- **Send Email**: MaaS360 will send them an email telling them about the new app

5. When you have finished selecting the options you want, click **Add**.

Note: *The Secure Productivity Suite offers many more options for securing apps. For more information, contact your account representative.*

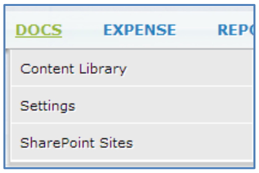
Documents

The Document Management features of MaaS360 are accessed from the **Docs** tab.

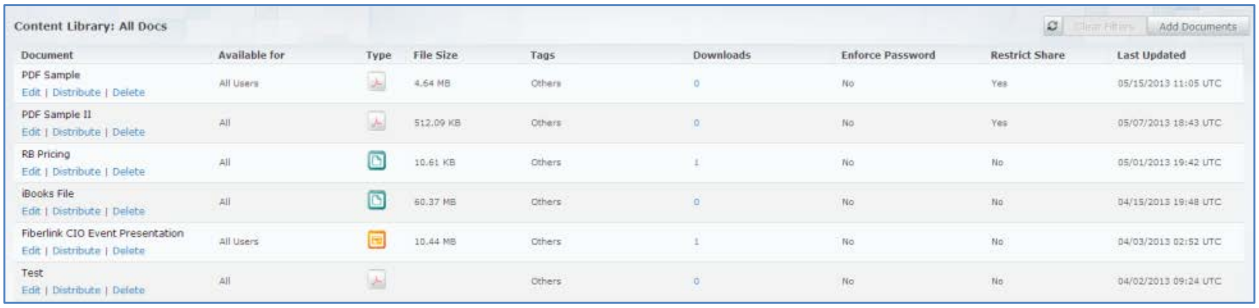
Content Library

MaaS360 allows you to distribute documents and files to your users quickly and easily. Each document must be loaded into the MaaS360 Content Library before it can be distributed.

To access the Content Library, mouse over **Docs** and click **Content Library**.



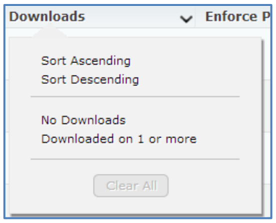
The Content Library lists your files and provides basic information about them.


Content Library: All Docs

Document	Available for	Type	File Size	Tags	Downloads	Enforce Password	Restrict Share	Last Updated
PDF Sample Edit | Distribute | Delete	All Users		4.64 MB	Others	0	No	Yes	05/15/2013 11:05 UTC
PDF Sample II Edit | Distribute | Delete	All		512.09 KB	Others	0	No	Yes	05/07/2013 18:43 UTC
RB Pricing Edit | Distribute | Delete	All		10.61 KB	Others	1	No	No	05/01/2013 19:42 UTC
iBooks File Edit | Distribute | Delete	All		60.37 MB	Others	0	No	No	04/15/2013 19:48 UTC
Fiberlink CIO Event Presentation Edit | Distribute | Delete	All Users		10.44 MB	Others	1	No	No	04/03/2013 02:52 UTC
Test Edit | Distribute | Delete	All			Others	0	No	No	04/02/2013 09:24 UTC

Click the highlighted number under **Downloads** to see the devices that have downloaded the file.

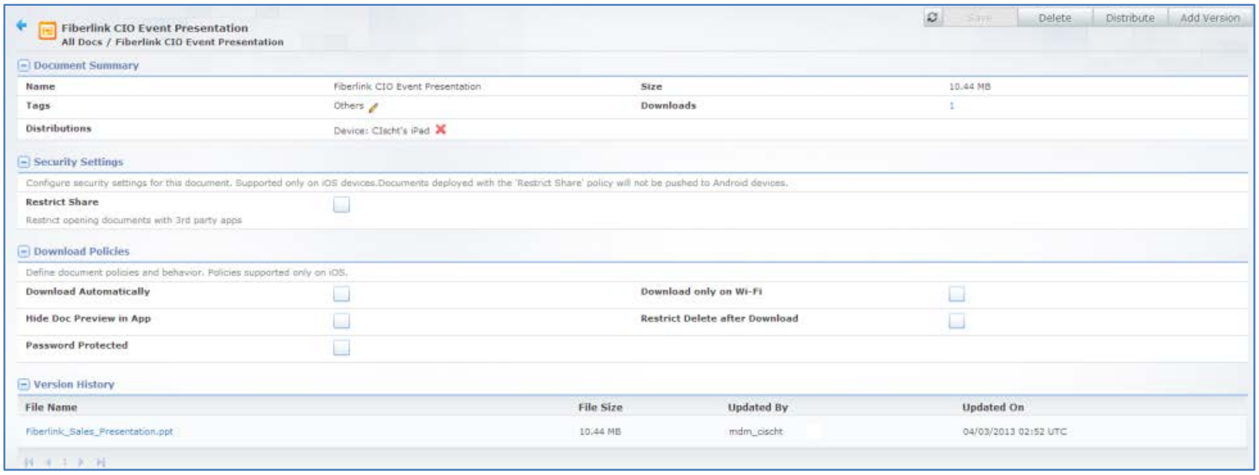
You can sort and filter your files by clicking on the column headings.



There are links under each app you can use to take action.

Edit

Click the **Edit** link to see detailed information about the app.



Fiberlink CIO Event Presentation
All Docs / Fiberlink CIO Event Presentation

Document Summary

Name	Fiberlink CIO Event Presentation	Size	10.44 MB
Tags	Others	Downloads	1
Distributions	Device: CIscht's iPad ✕		

Security Settings

Configure security settings for this document. Supported only on iOS devices.Documents deployed with the 'Restrict Share' policy will not be pushed to Android devices.

Restrict Share ☐
Restrict opening documents with 3rd party apps

Download Policies

Define document policies and behavior. Policies supported only on iOS.

Download Automatically	☐	Download only on Wi-Fi	☐
Hide Doc Preview in App	☐	Restrict Delete after Download	☐
Password Protected	☐		

Version History

File Name	File Size	Updated By	Updated On
Fiberlink_Sales_Presentation.ppt	10.44 MB	mdm_cischt	04/03/2013 02:52 UTC

You can see information about the distribution, including the size of the file and any security that has been applied to it. You can also see the version history for the file. Click the red **X** to delete a distribution.

For iOS devices, you can select **Restrict Share** and prevent documents from being opened with third-party apps. On Android devices it will prevent the content from going to the device.

You can also specify the download policies for iOS devices:

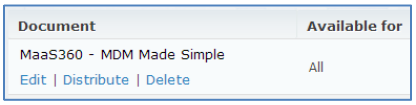
- **Download Automatically**: The document will automatically be downloaded onto the device
- **Hide Doc Preview in App**: A preview of the document will not be shown. This is for file formats like iBooks where preview is not supported
- **Password Protected**: Users must enter a password to access the document
- **Download only on Wi-Fi**: To reduce mobile data costs, the document will only be downloaded on a Wi-Fi network
- **Restrict Delete after Download**: Prevents users from removing a locally cached copy of the document

After making your changes, click **Save**.

You can also remove the document from the Content Library by clicking **Delete** from this screen.

Distribute

To distribute a document, click the **Distribute** link under its name.

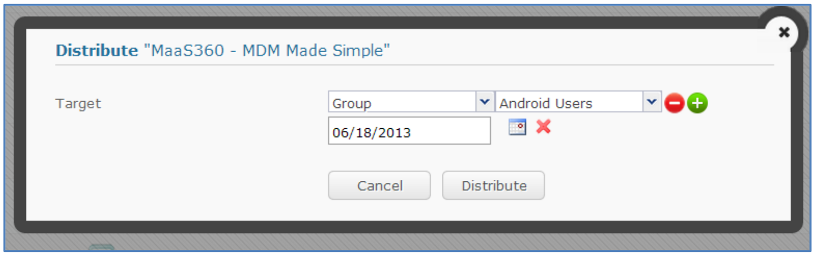


Document	Available for
MaaS360 - MDM Made Simple Edit | Distribute | Delete	All

Specify if an individual device, a group or all users should receive the document. If you want to distribute the document to more than one target, click ⊕.

You can also enter an expiration date when MaaS360 will remove the document from an individual device, a group or all users.

Click **Distribute**.



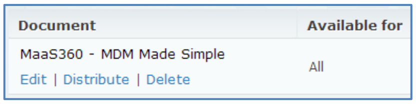
Distribute "MaaS360 - MDM Made Simple"

Target: Group | Android Users

06/18/2013

Delete

To delete a document, click the Delete link under its name.

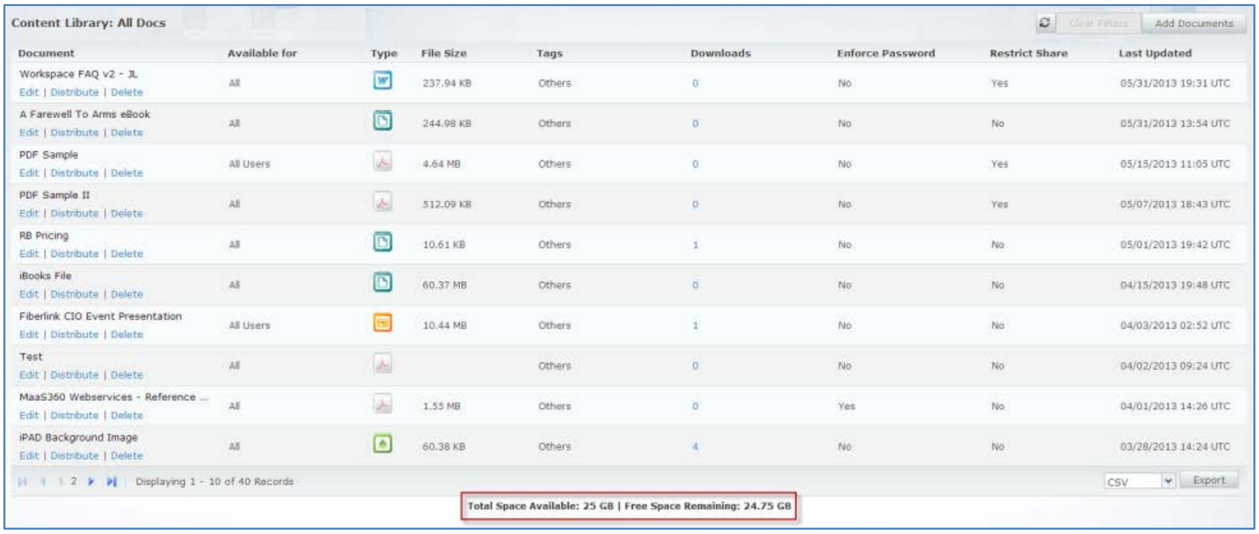


Document	Available for
MaaS360 - MDM Made Simple Edit | Distribute | Delete	All

Adding Documents to the Content Library

If you wish to add a new document, mouse over **Docs** and select **Content Library**.

At the bottom of the page you can see how much free space is still available—you may need to delete documents before you can add the new one.



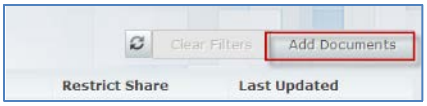
Content Library: All Docs

Document	Available for	Type	File Size	Tags	Downloads	Enforce Password	Restrict Share	Last Updated
Workspace FAQ v2 - JL Edit | Distribute | Delete	All	W	237.94 KB	Others	0	No	Yes	05/31/2013 19:31 UTC
A Farewell To Arms eBook Edit | Distribute | Delete	All		244.98 KB	Others	0	No	No	05/31/2013 13:54 UTC
PDF Sample Edit | Distribute | Delete	All Users		4.64 MB	Others	0	No	Yes	05/15/2013 11:05 UTC
PDF Sample II Edit | Distribute | Delete	All		512.09 KB	Others	0	No	Yes	05/07/2013 18:43 UTC
RB Pricing Edit | Distribute | Delete	All		10.61 KB	Others	1	No	No	05/01/2013 19:42 UTC
iBooks File Edit | Distribute | Delete	All		60.37 MB	Others	0	No	No	04/15/2013 19:48 UTC
Fiberlink CIO Event Presentation Edit | Distribute | Delete	All Users		10.44 MB	Others	1	No	No	04/03/2013 02:52 UTC
Test Edit | Distribute | Delete	All			Others	0	No	No	04/02/2013 09:24 UTC
MaaS360 Webservices - Reference ... Edit | Distribute | Delete	All		1.55 MB	Others	0	Yes	No	04/01/2013 14:26 UTC
iPAD Background Image Edit | Distribute | Delete	All		60.38 KB	Others	4	No	No	03/28/2013 14:24 UTC

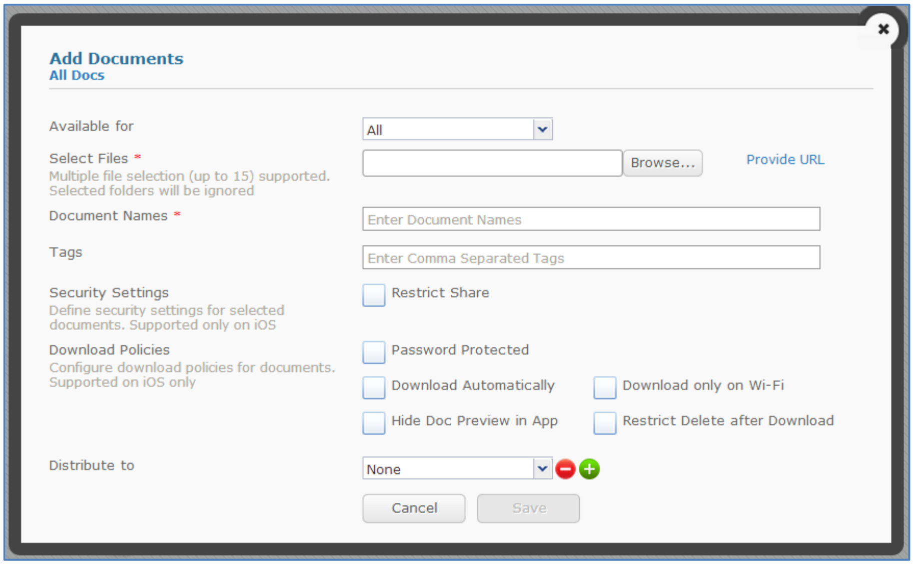
1 2 | Displaying 1 - 10 of 40 Records

Total Space Available: 25 GB | Free Space Remaining: 24.75 GB

Click the **Add Documents** button to upload documents that you wish to distribute to iOS and Android mobile devices.



Enter the details about the document.



Add Documents
All Docs

Available for: All

Select Files *
Multiple file selection (up to 15) supported. Selected folders will be ignored

Document Names *: Enter Document Names

Tags: Enter Comma Separated Tags

Security Settings
Define security settings for selected documents. Supported only on iOS
□ Restrict Share

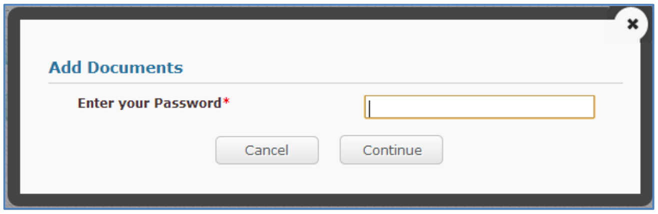
Download Policies
Configure download policies for documents. Supported on iOS only
□ Password Protected
□ Download Automatically □ Download only on Wi-Fi
□ Hide Doc Preview in App □ Restrict Delete after Download

Distribute to: None

Available for	Specify the group that can receive the document.
Select Files	Browse to the file you want to add and select it. You can upload up to 15 files at a time.
Document Names	Enter the name you want your users to see.
Tags	Enter tags to help your users find the document, separated by a comma.
Security Settings	Click **Restrict Share** if you want to prevent users from opening the document with a third-party app.
Download Policies	Specify the policies that apply to this document: • **Password Protected**: Users must enter a password to access the document • **Download Automatically**: The document will automatically be downloaded onto the device • **Hide Doc Preview in App**: A preview of the document will not be shown for file formats like iBooks where preview is not supported • **Download only on Wi-Fi**: To reduce costs, the document will only be downloaded on a Wi-Fi network • **Restrict Delete after Download**: Prevents users from removing a locally cached copy of the document
Distribute to	Specify if the document should immediately be distributed to all devices and users, a specific group, a specific device, or if it should not be distributed immediately (**None**). You can also enter an expiration date when the document will be removed from an individual device, a group or all users.

Click **Save**.

When prompted, enter your password and click **Continue**.

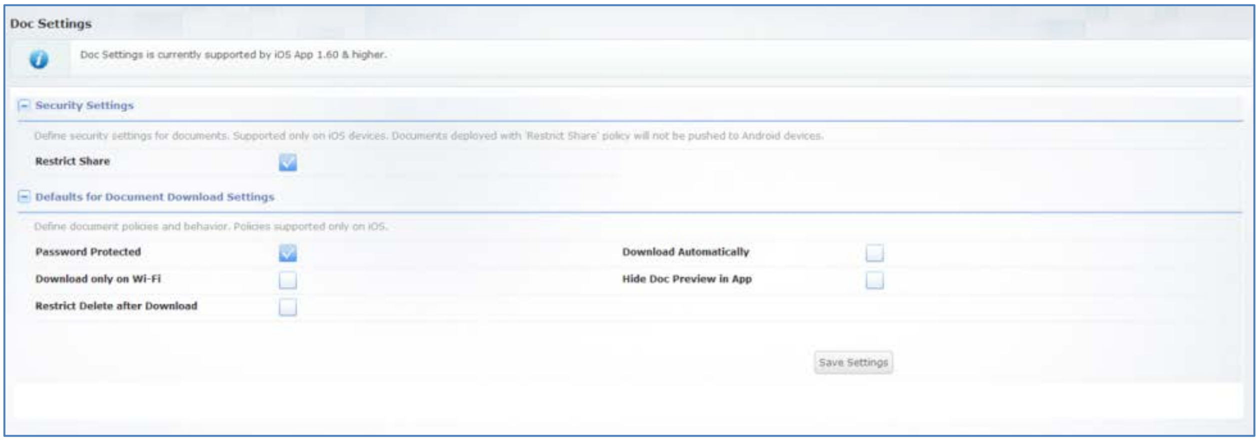


Add Documents

Enter your Password*

Document Settings

Select **Docs** > **Settings** to specify document policies and behavior.



Doc Settings

Doc Settings is currently supported by iOS App 1.60 & higher.

Security Settings

Define security settings for documents. Supported only on iOS devices. Documents deployed with 'Restrict Share' policy will not be pushed to Android devices.

Restrict Share ☑

Defaults for Document Download Settings

Define document policies and behavior. Policies supported only on iOS.

Password Protected ☑ Download Automatically ☐

Download only on Wi-Fi ☐ Hide Doc Preview in App ☐

Restrict Delete after Download ☐

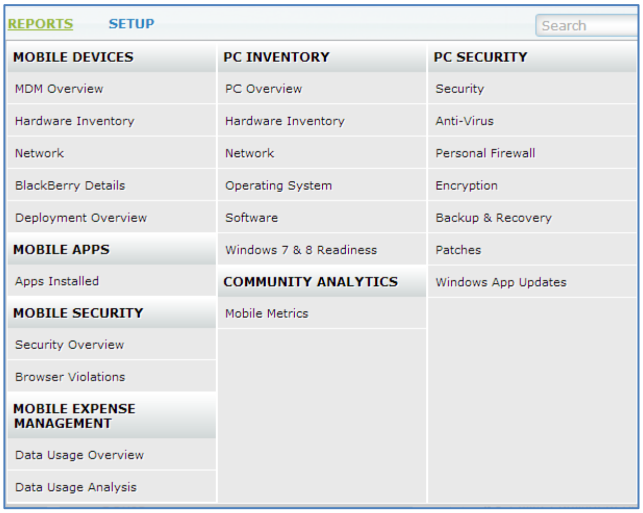
Restrict Share	Users cannot open documents with third-party apps, email documents, or copy/paste the content.
Password Protected	Users must enter a passcode to access the document.
Download only on Wi-Fi	To reduce costs, the document will only be downloaded on a Wi-Fi network.
Restrict Delete after Download	Prevents users from removing a locally cached copy of the document.
Download Automatically	The document will automatically be downloaded onto the device.
Hide Doc Preview in App	A preview of the document will not be shown for file formats like iBooks where preview is not supported.

These are the default settings for all your documents.

Reports

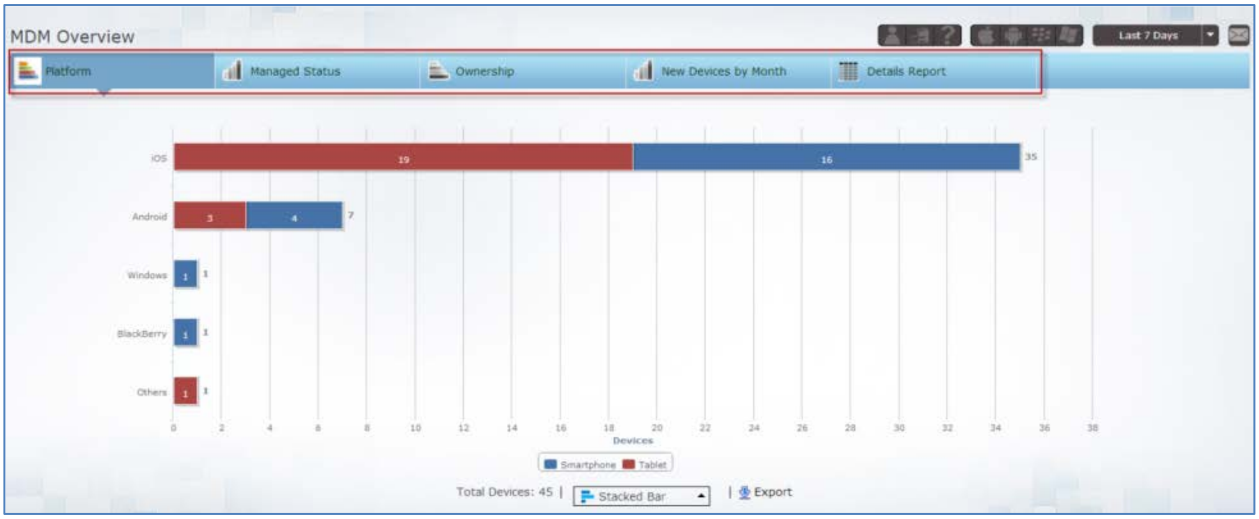
MaaS360 Mobile Intelligence™ reports allows you to use enhanced reporting functions, such as the tabular presentation of reports to group associated graphs and reports, and to provide easy navigation between the reports. It also includes filters, which help you generate a variety of real-time reports or narrow down report details based on your filter criteria.

To access the reports, mouse over the Reports tab and select the report family you want.



Note: *The reports that appear on the* ***Reports*** *tab depend on the products you have purchased. The list you see may be different than what is shown in this document.*

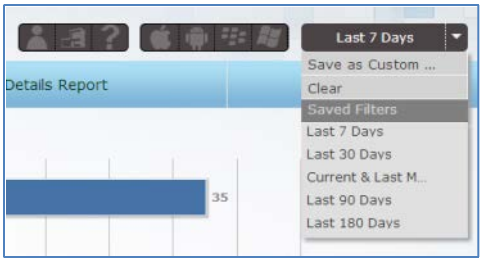
Separate reports in each family appear on tabs.



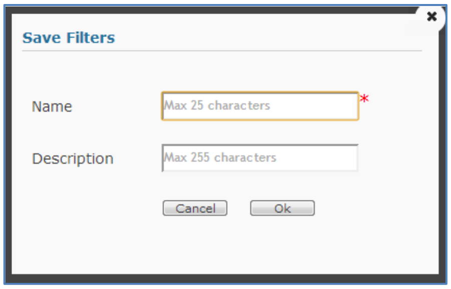
There are filters at the screen to help you manage your data:

- Personal

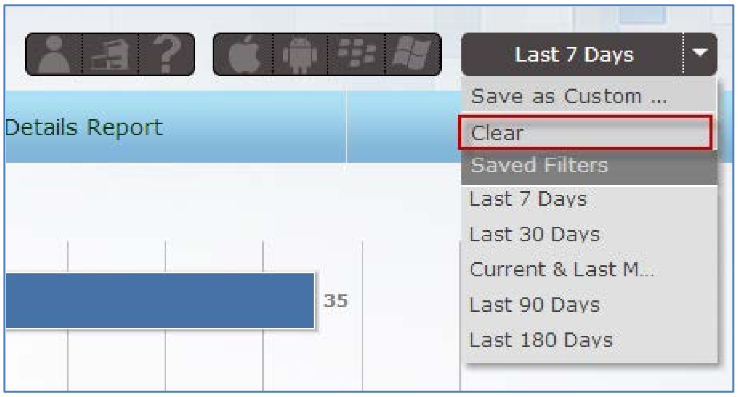
- Corporate owned
- Unspecified
- iOS
- Android
- BlackBerry
- Windows Phone
- Time period



You can save your filter so you can use it again. Click **Save as Custom**, and then enter a name and description for it.



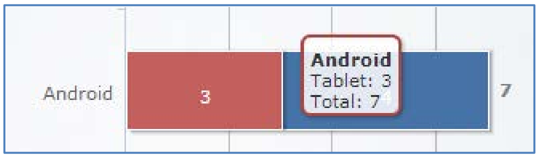
Note: *The filter you select for one report in a family is retained for the other reports until you clear it by clicking* ***Clear*** *on the pull-down menu.*



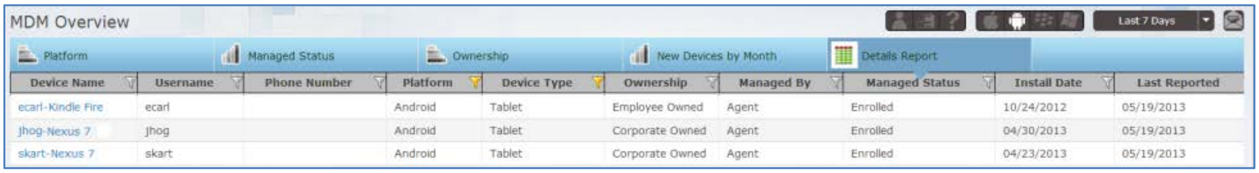
You can subscribe to reports by clicking ✉.

You can specify the graphs and reports included in the subscription, the format (PDF or PPT), the email recipients, the delivery frequency and more.

You can mouse over part of a graph to see the details about it. For example, the following shows that out of the 7 Android devices, 3 are tablets:



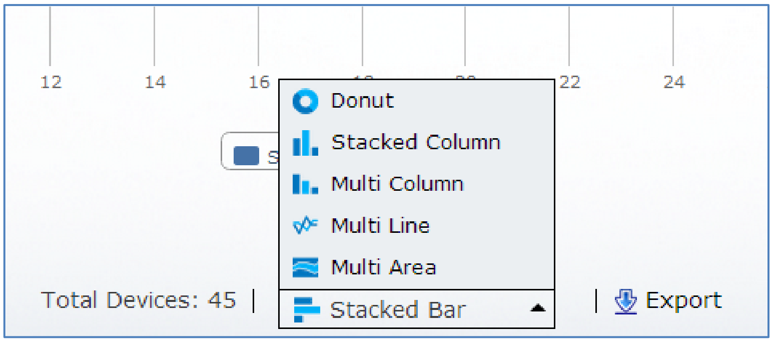
If you click on it, MaaS360 displays the **Details Report** filtered to show information about those tablets:



Device Name	Username	Phone Number	Platform	Device Type	Ownership	Managed By	Managed Status	Install Date	Last Reported
ecarl-Kindle Fire	ecarl		Android	Tablet	Employee Owned	Agent	Enrolled	10/24/2012	05/19/2013
jhog-Nexus 7	jhog		Android	Tablet	Corporate Owned	Agent	Enrolled	04/30/2013	05/19/2013
skart-Nexus 7	skart		Android	Tablet	Corporate Owned	Agent	Enrolled	04/23/2013	05/19/2013

The active filters are highlighted (yellow) for the associated columns.

You can choose the type of chart by selecting it from the menu at the bottom of the page.



You can also download the report by clicking **Export**.